

FORM PTO-1390 (Modified) (REV 11-2000)		U.S. DEPARTMENT OF COMMERCE PATENT AND TRADEMARK OFFICE		ATTORNEY'S DOCKET NUMBER <b>(H)01PH0419USP</b>	
<b>TRANSMITTAL LETTER TO THE UNITED STATES</b> <b>DESIGNATED/ELECTED OFFICE (DO/EO/US)</b> <b>CONCERNING A FILING UNDER 35 U.S.C. 371</b>				U.S. APPLICATION NO. (IF KNOWN, SEE 37 CFR) <div style="font-size: 1.5em; font-weight: bold; text-align: center;">10/018721</div>	
INTERNATIONAL APPLICATION NO <b>PCT/DE00/01901</b>		INTERNATIONAL FILING DATE <b>16 June 2000</b>		PRIORITY DATE CLAIMED <b>17 June 1999</b>	
TITLE OF INVENTION <b>Safety Related Automation Bus System</b>					
APPLICANT(S) FOR DO/EO/US <b>Karsten Meyer-Gräfe</b>					
Applicant herewith submits to the United States Designated/Elected Office (DO/EO/US) the following items and other information: <ol style="list-style-type: none"> <li>1. <input checked="" type="checkbox"/> This is a <b>FIRST</b> submission of items concerning a filing under 35 U.S.C. 371.</li> <li>2. <input type="checkbox"/> This is a <b>SECOND</b> or <b>SUBSEQUENT</b> submission of items concerning a filing under 35 U.S.C. 371.</li> <li>3. <input type="checkbox"/> This is an express request to begin national examination procedures (35 U.S.C. 371(f)). The submission must include items (5), (6), (9) and (24) indicated below.</li> <li>4. <input type="checkbox"/> The US has been elected by the expiration of 19 months from the priority date (Article 31).</li> <li>5. <input checked="" type="checkbox"/> A copy of the International Application as filed (35 U.S.C. 371 (c) (2))             <ol style="list-style-type: none"> <li>a. <input checked="" type="checkbox"/> is attached hereto (required only if not communicated by the International Bureau);</li> <li>b. <input checked="" type="checkbox"/> has been communicated by the International Bureau;</li> <li>c. <input type="checkbox"/> is not required, as the application was filed in the United States Receiving Office (RO/US).</li> </ol> </li> <li>6. <input checked="" type="checkbox"/> An English language translation of the International Application as filed (35 U.S.C. 371(c)(2)).             <ol style="list-style-type: none"> <li>a. <input checked="" type="checkbox"/> is attached hereto.</li> <li>b. <input type="checkbox"/> has been previously submitted under 35 U.S.C. 154(d)(4).</li> </ol> </li> <li>7. <input type="checkbox"/> Amendments to the claims of the International Application under PCT Article 19 (35 U.S.C. 371 (c)(3))             <ol style="list-style-type: none"> <li>a. <input type="checkbox"/> are attached hereto (required only if not communicated by the International Bureau).</li> <li>b. <input type="checkbox"/> have been communicated by the International Bureau.</li> <li>c. <input type="checkbox"/> have not been made; however, the time limit for making such amendments has NOT expired.</li> <li>d. <input type="checkbox"/> have not been made and will not be made.</li> </ol> </li> <li>8. <input type="checkbox"/> An English language translation of the amendments to the claims under PCT Article 19 (35 U.S.C. 371(c)(3)).</li> <li>9. <input checked="" type="checkbox"/> An oath or declaration of the inventor(s) (35 U.S.C. 371 (c)(4)). <b>UNEFFECTED</b></li> <li>10. <input checked="" type="checkbox"/> An English language translation of the annexes to the International Preliminary Examination Report under PCT Article 36 (35 U.S.C. 371 (c)(5)).</li> <li>11. <input checked="" type="checkbox"/> A copy of the International Preliminary Examination Report (PCT/IPEA/409).</li> <li>12. <input checked="" type="checkbox"/> A copy of the International Search Report (PCT/ISA/210).</li> </ol> <p><b>Items 13 to 20 below concern document(s) or information included:</b></p> <ol style="list-style-type: none"> <li>13. <input checked="" type="checkbox"/> An Information Disclosure Statement under 37 CFR 1.97 and 1.98.</li> <li>14. <input type="checkbox"/> An assignment document for recording. A separate cover sheet in compliance with 37 CFR 3.28 and 3.31 is included.</li> <li>15. <input checked="" type="checkbox"/> A <b>FIRST</b> preliminary amendment.</li> <li>16. <input type="checkbox"/> A <b>SECOND</b> or <b>SUBSEQUENT</b> preliminary amendment.</li> <li>17. <input checked="" type="checkbox"/> A substitute specification.</li> <li>18. <input type="checkbox"/> A change of power of attorney and/or address letter.</li> <li>19. <input type="checkbox"/> A computer-readable form of the sequence listing in accordance with PCT Rule 13ter.2 and 35 U.S.C. 1.821 - 1.825.</li> <li>20. <input type="checkbox"/> A second copy of the published international application under 35 U.S.C. 154(d)(4).</li> <li>21. <input type="checkbox"/> A second copy of the English language translation of the international application under 35 U.S.C. 154(d)(4).</li> <li>22. <input checked="" type="checkbox"/> Certificate of Mailing by Express Mail</li> <li>23. <input checked="" type="checkbox"/> Other items or information:</li> </ol> <p style="margin-top: 10px;"> <b>General Authorization to Charge Fees</b>  <b>5 Sheets of formal drawings</b> </p>					

Page 2 of 2

10/018721

Applicant Meyer-Grafe  
Attorney Docket (H)01PH0419USP  
PCT/DE00/01901

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

531 Rec'd PCT/PTC 14 DEC 2001

Re: International Application PCT/DE00/01901  
Filed June 16, 2000  
Title Safety-related automation bus system  
Applicant Meyer-Grafe  
Attorney Docket (H)01PH0419USP

Box PCT  
Commissioner for Patents  
Washington, DC 20231

Preliminary Amendment

Dear Sir or Madam:

Please amend the above-identified application as follows:

In the Specification: A substitute specification and "Version with Markings to show Changes Made" is included herewith.

In the Claims:

Please cancel claims 1-31 of the Annexes and substitute the following new claims 32-66.

32. An automation system (1), comprising at least  
a bus (2),  
I/O bus subscribers (31-38) connected to the bus (2),  
a standard control device (4; 40, 41),  
at least one safety analyzer (5, 5', 5'') which monitors data flow via the bus system and is  
designed to carry out at least one safety-related function,  
wherein the safety analyzer is at least one of set up for checking and processing safety-  
related data in a bus datastream and having a device for manipulating the datastream transmitted  
on the bus (2).

33. The automation system (1) as claimed in claim 32, wherein the standard control device controls at least one safety-related output.
34. The automation system (1) as claimed in claim 32,  
wherein the safety analyzer (5, 5', 5'') has a freely programmable logic device, which processes monitored safety-related data.
35. The automation system (1) as claimed in claims 32,  
wherein the safety analyzer (5, 5', 5'') is not a logic bus subscriber in the automation system (1) and has at least one safety-related output (6) via which at least one bus subscriber (31-38) which is associated with the safety analyzer of the automation system is switched on or off.
36. The automation system (1) as claimed in claim 35,  
wherein the safety analyzer (5, 5', 5'') is set up for switching off at least one of a safety island, a bus spur (8), and the entire automation system.
37. The automation system (1) as claimed in claim 32,  
wherein the safety analyzer (5') has at least one safety-related input (10), via which the safety analyzer is connected to a safety-related device (11) in the automation system for detecting safety-related data.
38. The automation system (1) as claimed in claim 32,  
wherein the bus (2) is connected via an interface assembly (41) to a host (40), with the process-related control being arranged in the host, and the safety-related control being arranged in the interface assembly.
39. The automation system (1) as claimed in claim 32,  
wherein the bus (2) is a serial bus, and at least one safety analyzer (5, 5') is arranged in a long-distance bus section of the automation system.

40. The automation system (1) as claimed in claim 38,  
wherein a safety analyzer (5) is one of arranged directly after the host (40) or arranged after the interface assembly (41).
41. The automation system (1) as claimed in claim 38,  
wherein a safety analyzer (5) is arranged in the interface assembly (41).
42. The automation system (1) as claimed in claim 32,  
wherein the safety analyzer (5, 5', 5'') comprises a memory device for storing a process map.
43. The automation system (1) as claimed in claim 32,  
wherein the safety analyzer (5, 5', 5'') has a device for manipulating at least one of input data and output data transmitted on the bus (2).
44. The automation system (1) as claimed in claim 43,  
wherein the device overwrites at least one of the input and output data in the safety analyzer (5, 5', 5'').
45. The automation system (1) as claimed in claim 43, wherein the device inserts data into the datastream.
46. The automation system (1) as claimed in claim 32,  
wherein at least one safety analyzer (5, 5', 5'') is of redundant design.
47. A method for operating an automation system (1) as claimed in claim 32, comprising the following steps:  
using a standard control device (4; 40, 41) for carrying out a process control with the processing of process-linked I/O data and safety-related data, and

carrying out processing of safety-related data in at least one safety analyzer (5, 5', 5'')  
with safety-related logic linking data in the bus datastream being processed in the safety  
analyzer.

48. The method as claimed in claim 47,  
further comprising the step of using the standard control device to control at least one  
safety-related output.

49. The method as claimed in claim 47,  
further comprising the step of comparing the safety-related logic linking data, which is  
transmitted via the bus, for at least one of the standard control device (4, 41) and at least one  
further safety analyzer (5, 5', 5'') with the corresponding logic linking data of the first safety  
analyzer, in a safety analyzer (5, 5', 5'').

50. The method as claimed in claim 47,  
further comprising the step of checking the logic linking data, which is produced by the  
standard control (4, 41) and is sent as output data via the bus in at least one safety analyzer (5, 5',  
5'') by modeling the safety-related logic links of the standard control (4, 41).

51. The method as claimed in claim 49,  
further comprising carrying out safety-related functions in response to the comparison by  
the safety analyzer (5, 5', 5'').

52. The method as claimed in claim 50,  
further comprising carrying out safety-related functions in response to the checking by  
the safety analyzer.

53. The method as claimed in claim 47, further comprising the step of carrying-out a safety-  
related function via a safety-related output (6) of the safety analyzer (5, 5', 5'').

54. The method as claimed in claim 47,  
further comprising the step of using the safety analyzer to carry out safety-related functions in response to the safety-related data detected via the safety-related input (10) of the safety analyzer (5').
55. The method as claimed in claim 54,  
wherein the process of carrying out the safety-related function comprises switching a bus subscriber (32-38) on or off.
56. The method as claimed in claim 47,  
wherein the safety analyzer (5, 5', 5'') at least one of overwrites or deletes at least one data item into the datastream and inserts at least one data item into the bus datastream by means of a device for manipulating the datastream on the bus (2).
57. The method as claimed in claim 56,  
wherein the safety analyzer (5, 5', 5'') at least partially stores the monitored datastream and copies input data in the bus datastreams to output data in the bus datastream, and vice versa.
58. The method as claimed in claim 47,  
wherein safety-related data is transmitted via the bus (2) using a security protocol.
59. The method as claimed in claim 58,  
wherein in addition to the safety data item, the security protocol comprises at least one of the negated safety data item, a sequential number, an address and data protection information (CRC).
60. The method as claimed in claim 47,

61. The method as claimed in claim 60,

62. The method as claimed in claim 47,

64. The method as claimed in claim 47,

65. The method as claimed in claim 47,

66. The method as claimed in claim 47,

6

Applicant Meyer-Grafe  
Attorney Docket (H)01PH0419USP  
PCT/DE00/01901

Remarks

This Preliminary Amendment removes multiple dependencies from the claims and conforms the claims to US style and practice. Please calculate the Filing Fee according to this Preliminary Amendment.

Respectfully submitted,



M. Robert Kestenbaum  
Reg. No. 20,430  
11011 Bermuda Dunes NE  
Albuquerque, NM USA 87111  
Telephone (505) 323-0771  
Facsimile (505) 323-0865

ENGLISH

TRANSLATION

10014721 0412202

10/018721

531 Rec'd PCT/7. 14 DEC 2001

01PH 0419USP

Phoenix Contact GmbH & Co

5/19/05

Safety-related automation bus system

The invention relates to a safety-related automation bus system as claimed in the precharacterizing clause of claim 1, and to a method for operating such a system.

Control and data transmission systems have gained a dominant position not only in industrial manufacturing owing to the high level of automation that they make possible. Such automation systems generally have at least sections or components in which more stringent requirements with respect to safety may be placed. For example, it is necessary to ensure that certain machines are operated within predetermined operating parameters, or it is necessary to prevent a machine from running even though someone is located in its operating area. In this context, for example, a lathe must not exceed a predetermined rotation speed or there must not be anyone in the radius of action of a robot, when that robot is being operated. Furthermore, when operating an automation system, it is necessary to ensure that, if one component in the system fails, the system does not change to an undefined, and hence unpredictable, state.

On approach to this problem according to the prior art is, in particular, to use a number of channels for the safety-relevant components in the system, that is to say to design them to be redundant. For example, safety bus components, that is to say for example bus subscribers which are associated with a safety-relevant machine, may be duplicated in an automation bus

system. At the same time, the central control and the bus may have a number of channels, or even a specific safety control system, which is separate from the process control system and in some circumstances is of redundant design, for controlling the safety-relevant components. This safety control system essentially carries out the logic links on the safety-related input information and then transmits, for example via an automation bus, safety-related logic linking data to output components. The output components themselves process the received safety measures and, if the test result is positive, output this to the peripherals. Furthermore, they switch their outputs to a safe state if they find a fault, or have no longer received any valid data within a predetermined time period.

The use of two control systems in the system, that is to say a process control system and the described safety control system, results in a number of disadvantages, however. Among other factors, the increasingly stringent requirements for the reaction time of automation systems means that such a system often has to be subdivided between safety islands. Furthermore, synchronization problems occur especially in multichannel control systems which, despite the system in principle being intact, can lead to failures or even to destruction of machine parts. Furthermore, the multichannel design results in an increase in the system and maintenance costs, due to the increased hardware complexity.

DE 198 15 150 A1 discloses a system which comprises an evaluation unit which is connected to the bus, continuously monitors the symbols transmitted via the bus system, and starts up a piece of equipment only when codings which are transmitted via the bus system are identified without any errors. To this end, the input data sent by the bus subscriber to the master is

evaluated, and the piece of equipment is switched on or off in response to the evaluation.

Such an approach is not as costly as the system described first, but it is highly inflexible in terms of upgrading the system or matching the system to other bus components.

Furthermore, the evaluation unit has sole responsibility for initiating a safety-based function, so that it is absolutely essential for the evaluation unit to be of redundant design in order to comply with stringent safety requirements.

One object of the invention is thus to provide a safety-related automation bus system which requires as little hardware redundancy as possible, and which can be flexibly matched to the respective requirements.

The invention solves this problem by means of an automation bus system having the features of claim 1 and a method for operating such a control and data processing system as claimed in claim 14. Developments of the invention are specified in the dependent claims.

According to the invention, the automation system comprises a bus system, sensor and actuator bus subscribers connected to it, and a standard control device which carries out the process control function with the processing of process-linked I/O data and safety-related control function with the processing of safety-related data, that is to say the control of safety-related inputs and outputs. It also includes what is referred to as a safety analyzer, which is connected to the bus by means of an appropriate interface and monitors the data flow via the bus, with the analyzer being set up to carry out safety-related functions. This relates, for example, to the actuation of a contractor for switching off the supply voltage to system components, or to the determination of the quality data. Such

quality data may include general system parameters, for example data on the occurrence of faults in system components, or bus transmission errors. The automation system is distinguished by the fact that the standard control device drives at least one  
5 safety-related output via the bus, but it may itself have such a safety-related output. According to the invention, a safety-related output denotes a sink for safety information which starts safety-based sequences as a function of the information, for example slowing down a machine or even switching off a machine by  
10 interrupting the supply power. The safety analyzer in the automation system according to the invention is designed for checking and/or for processing safety-related data, in particular safety-related logic linking data, in the bus datastream. In this case, safety-related logic linking data, for example data which  
15 the safety-related control system sends to safety-related outputs after processing safety-related data.

A system is therefore provided which can be matched extremely flexibly to the respective requirements for the automation system. For example, each safety bus component may be  
20 allocated such a safety analyzer, and a safety analyzer may itself also be integrated in the safety component, for example a safety bus subscriber, although it is also possible for one individual safety analyzer to carry out the processing of safety-related data or the checking of safety-related logic linking data  
25 in the bus datastream for a number of safety bus components, or even for all the safety bus components in the system.

The principle of the invention is based in the inventor's experience on the fact that the electronics used in present-day automation systems themselves fail only rarely. The integration  
30 of the present-day digital safety technology in automation technology in the form of safety control systems or safety bus

systems according to the prior art frequently have the disadvantage of decreasing the system availability. In order to reduce the down times, availability structures are therefore also used in addition to said safety components, but they themselves  
5 lead to a not inconsiderable increase in costs, due to the increased hardware complexity.

The invention is therefore based on the reliability of present-day automation systems, and integrates pure emergency electronics or software, which become actively involved in the  
10 operation of the system only when the standard technology is operating incorrectly. The standard control device therefore also processes safety-related data, that is to say it controls safety-relevant inputs and outputs. In particular, the safety-related logic linking data which is produced in the bus datastream is,  
15 however, monitored and checked by the safety analyzer. This has the advantage for the user that it is no longer absolutely necessary to maintain strict isolation between the circuit technology and the standard technology during programming. The automation system according to the invention can be used on all  
20 systems with a bus, in particular on bus systems using master-slave bus access methods. Independently of the arrangement of the safety analyzer in the long-distance bus section, this safety analyzer can read all the IN data on the bus, in, for example, a serial bus system in accordance with EN 50 254, but the amount of  
25 OUT data which can be monitored depends on the arrangement of the safety analyzer in the system. The expression bus datastream in this case, according to the invention, refers to all the information that is transmitted via the bus, in particular including data transported via the bus in a sum frame.

30 In order to comply with the relevant safety requirements, the safety analyzer can initiate the necessary safety-related

functions in response to the checking and/or the processing of safety-related data, in particular of logic linking data in the bus datastream. In this case, the safety analyzer can react not only to OUT data, that is to say logic linking data from the standard control device, but also to IN data, that is to say to information in the bus datastream, which has been sent from individual I/O bus subscribers to the standard control device.

In order to identify an error in safety-related logic linking data which is transported via the bus, the safety analyzer may have a fully programmable logic device, in which the monitored data, in particular the monitored safety-related data, is processed. In this way, by modeling the safety-related logic links of the standard control system, the safety analyzer can check the logic linking data of this control system sent as OUT data via the bus, and can carry out the necessary safety-related functions in response to the check or the comparison. In order, for example, to change the system to a safe state, the safety analyzer may have an output via which an assembly in particular a bus subscriber in the automation system, can be switched on or off. The switching-off process can be carried out by disconnection from the voltage supply. In order to change all the associated and mutually independent bus subscribers to a safe state, the safety analyzer may be set up for switching off a bus spur, a safety island comprising a number of mutually associated bus subscribers, or to switch off components on the basis of interlocking logic stored in the analyzer. However, it is also possible for the entire system to be disconnected from the voltage supply via the safety-related output of the safety analyzer.

In addition to monitoring the bus, the safety analyzer can also detect safety-related information via a direct input, by

means of which the safety analyzer is connected to a safety-related device in the automation bus system. In this case, this device may be, but need not be, connected to the bus. By way of example, the safety-related information accessible in this way  
5 includes the instantaneous rotation speed of the lathe already mentioned, with the analyzer output switching off the machine if a predetermined limiting rotation speed is exceeded.

In order to separate the safety-related information and the process data in the system, and in particular in the control  
10 system, the bus system may be connected via an interface assembly to a host, with the process-related control of the standard control device being arranged in the host, and the safety-related control of the standard control device being arranged in the interface assembly. The safety-related control system may, for  
15 example, advantageously be in the form of software functional modules, which carry out the necessary logic links on the safety-relevant I/O Information.

The safety-related control system can thus be implemented in the same way as the process control system. When coding the  
20 safety-related logic links, the programmer is independent of the programming language being used, in the same way as with the process control system.

The logic links in the safety analyzer have approximately the same scope as the logic links in the host and in the  
25 interface assembly, and can be produced either in the same programming language, or else in a different one. The safety analyzer also carries out a comparison of the logic links between the results from the host system and/or the interface assembly and its own results, and starts safety-based functions, for  
30 example in the event of an inequality.

The acceptance procedure for such a system can be carried

out considerably more easily than is the case with systems according to the prior art. The system can be started up with all the safety interlocks, without needing to switch the safety technology to be active. The necessary logic links are in this case located in the host system or in the interface assembly. The functionality of the system can be investigated first of all using a black-box test. In a second step, the safety technology is then connected, in the form of the safety analyzer or analyzers. Since only the safety logic links, but not the process data logic links, are present there, the white-box test can now be carried out quickly and clearly, thus allowing the acceptance times to be considerably reduced. Since the safety-related logic algorithms can also run on the host system and/or on the interface assembly, a comparison with those in the analyzer can be carried out quickly.

If the bus is a serial ring bus, for example a bus in accordance with EN 50254, and if a safety analyzer is arranged in the top-level long-distance bus section of the automation system, then this has access to all the IN data in the system since, in the system referred to, the data is carried in a forward transmission line and in a return transmission line by each bus subscriber. The analyzer is thus able to form a process map which is restricted to the IN data and the Out data to which it has access.

In bus systems with a linear topology, the safety analyzer can in general read all the information at any point in the bus system, and can thus produce a complete process map.

In one advantageous embodiment of the invention, the safety analyzer is arranged in a serial ring bus system directly after the host or the interface assembly, so that it can form a complete process map. The safety analyzer is thus able to check

and to process safety-based data, in particular safety-based logic linking data, for its correctness at any time and fully, since, in this case, the analyzer has access to all the In and Out data, that is to say all the input and output data.

5        If the safety analyzer is arranged in the interface assembly of the described serial ring bus system, then the function of the safety analyzer can be carried out by means of a software component in the interface assembly. The interface assembly in this case advantageously has a safety-related output, in order to  
10        carry out appropriate safety-based functions, for example using a contactor to switch off a supply voltage.

      However, in one particular advantageous embodiment of the invention, such safety-based functions can be carried out by direct data manipulation of the bus datastream by means of the  
15        safety analyzer. The manipulation includes rewriting, adding, insertion or substitution both of OUT data and of IN data in the bus datastream. If the process map is known, the safety analyzer can thus influence the operation of the automation system according to the invention in a far-reaching form, and can thus  
20        ensure that the system can be kept in defined states at any time. The principle of data manipulation can furthermore also be used in order to make available bus datastream components which are generally not accessible in a safety analyzer arranged in the bus spur, in that a safety analyzer which is arranged in the long-  
25        distance bus converts the relevant data to data which is transported in the relevant bus spur. This provides a direct data link between safety analyzers.

      Data manipulation by means of a safety analyzer can also be used, in a bus system operating on the master-slave principle, in  
30        order to transmit data between at least two slaves, in particular between individual bus subscribers, by means of a point-to-point

link via at least one safety analyzer, with the safety analyzer copying data in the bus datastream. Depending on the position of the two slaves in the bus system, the master is in some circumstances not included in this data link, so that the data transportation takes place completely independently of the bus master. Such a data link between two slaves is, apart from this, also possible when the bus master is carrying out a copying function. While, when a safety analyzer is acting as an agent, as described above, the bus master is not included in the data transportation, at least in certain situations, the bus master is absolutely essential for the second form of point-to-point link between two slaves.

The interchanging of data between at least two slaves, for example between individual bus subscribers, by means of a point-to-point link can, furthermore, also be provided by including the master or the control system in the transmission, with the master or the control system in this case copying the data in the bus datastream.

In order to improve the data security, the safety-related data can also be transmitted via the bus using a security protocol. For example, the security protocol may include not only the safety data item but also the negated safety data item, a sequential number, an address and/or data protection information (CRC).

The flexibility of the system is evident in particular in a further advantageous embodiment of the invention, in which the automation system according to the invention has a number of safety analyzers, with safety-related logic links that are carried out in one safety analyzer being carried out in redundant form in at least one further safety analyzer, and the same safety functions being carried out and initiated, at least partially, by

both safety analyzers. In this case, the relevant safety analyzers can also carry out different safety-related logic links in addition to the redundant logic links, that is to say those which are carried out on both analyzers.

The invention will be explained in the following text by describing a number of embodiments based on the drawings, in which:

Fig. 1 shows an outline illustration of a first embodiment of the automation system according to the invention, with two safety analyzers in the long-distance bus system,

Fig. 2 shows an outline sketch of a further embodiment of the invention, with a safety analyzer being arranged directly after the interface assembly,

Fig. 3 shows the automation system according to the invention in the form of an outline sketch with a safety analyzer integrated in the interface assembly, and with a second safety analyzer at the head of a bus spur,

Fig. 4 shows an automation system according to the invention with two safety analyzers whose outputs are connected to one another,

Fig. 5 shows an outline block diagram illustration of a safety analyzer with various inputs and outputs, and

Figs. 6a and 6 show an outline illustration of data manipulation on the bus datastream by means of the safety analyzer.

Fig. 1 shows an outline illustration of the automation system 1 according to the invention, that is to say a control and data transmission system according to the invention. This has a bus 2 to which I/O bus subscribers with associated sensors and

actuators are connected. A standard control device 4 uses the bus for process control, processing process-linked I/O data. To do this, the controller 4 receives data from the individual bus subscribers 31 - 38, which in turn themselves receive data from the standard control device. Furthermore, the standard control device deals with the processing of safety-related data. In this sense, the standard control device carries out not only the process-linked inputs and outputs but also the processing of the safety-relevant inputs and outputs. According to the invention, a safety-related input denotes an information source, with the information emitted by the source being related to some way to the safety of the automation system according to the invention. By way of example, one such safety-related input is the rotation speed sensor of a lathe which is connected to the bus 2 via a bus subscriber 32, since the machine must not rotate at a speed above a predetermined limit. A further example of a safety-related input in the described embodiment of the invention is a photodetector of a light barrier, which is used to monitor the operating area of the lathe. In this case as well, the standard control device has access via the bus to the information at the safety-related input. After processing the safety-related data, for example in the form of a logic link, the control device 4 sends this safety-related logic linking data to safety-related outputs. By way of example, the standard control device may send a switch-off command for said lathe via the bus to the associated bus subscriber 32 when the maximum rotation speed has been exceeded and there is thus a risk of the system running out of control. In this case as well, the safety-related controller in the standard control device communicates via the bus with the safety-related output.

The automation system according to the invention also has

two safety analyzers 5, 5', each of which monitors the data flow via the bus system in real time by means of an interface. The safety analyzers are set for logic linking and/or processing of safety-related data in the bus datastream. This means that they  
5 can deal with the safety-related logic links of the standard control device, since they can access the safety-related data transported via the bus.

To this end, the safety analyzers 5, 5' each have a freely programmable logic device in which the monitored data, in  
10 particular the monitored safety-related data, is processed. By way of example, the safety analyzers 5, 5' can model the safety-related logic links of the standard control system to check their logic linking data sent via the bus as output data. In the present case, the safety-related logic links relate to an  
15 individual bus subscriber 32. In this case, the safety analyzer 5 is responsible for the safety-related inputs and outputs which are associated with this bus subscriber. In the embodiment of the invention illustrated in Fig. 1, the safety analyzers 5 and 5' are not logical bus subscribers in the automation system.

20 However, the safety analyzer 5 has a safety-related output 6 via which the bus subscriber 32 associated with the safety analyzer can be switched off. This is done by means of a circuit of a contactor 7, which disconnects the bus subscriber and the connected assemblies and machines from the supply voltage. In  
25 this way, the safety analyzer 5 carries out a safety-related function in response to the check or the comparison, in this case switching off the supply voltage. If, for example, a fault is identified in the safety-related logic linking data from the standard control device, the safety analyzer can switch off the  
30 relevant bus subscriber via the described output, since the safety-related controller provided by the standard control device

is no longer operating correctly. In a similar way, a bus subscriber is switched off if the safety-related controller does not send the required data to that bus subscriber and, in consequence, there is a risk of the system changing to an undefined state.

In the described embodiment, a local bus spur 8 with three bus subscribers 33, 34 and 35 is arranged via a bus coupler 9. These bus subscribers are dependent on the functionality and on the operation of the bus subscriber 32, which is associated with the safety analyzer 5. It is therefore necessary, when the bus subscriber 32 is switched off, for the bus subscribers on the local bus spur 8 to be disconnected from the supply voltage, as well. This interlocking logic is stored in the safety analyzer 5. A total of four bus subscribers must therefore be switched off, together with their subordinate assemblies and machines, as is illustrated schematically in Fig. 1 by means of a quadruple contactor 7.

The safety analyzer 5', like the first safety analyzer 5, is set up for monitoring the data transported via the bus. However, in contrast to the first safety analyzer 5, it does not have an input by means of which it can carry out safety-related functions. Instead of this, it has a safety-related input 10, via which the safety analyzer is connected to a safety-related device 11 in the automation system for detecting safety-related data. In the present case, this device 11 has a photodetector which, as part of a light barrier monitors the operating area of a welding robot. The sensor is not connected to the automation bus by means of a bus subscriber, but is connected directly to the safety analyzer 5'. In response to the safety-related data detected via the safety-related input 10 of the safety analyzer 5', the safety analyzer in this case also carries out a safety-related function.

If the photodetector 11 detects that someone has entered the operating area of the robot, then the safety analyzer 5' automatically switches off the corresponding bus subscriber 38 and its associated assemblies, and the robot. To do this, the safety analyzer 5' has a device for manipulating the input and output data transmitted to the bus. In this case, at least one data item in the datastream can be overwritten, deleted and/or at least one data item can be inserted into the bus datastream. Such a procedure is shown in Figs. 6a and 6. These Figs. show the amendment of input and output data for the standard control device 4 by the safety analyzer 5'. In both cases, an information unit 12 is read to a memory in the safety analyzer, and an information unit taken from another memory in the safety analyzer is then written to the corresponding point in the datastream. The bus subscriber and the assemblies connected to it, and hence the robot, can be switched off both via the manipulation of the input data and via the manipulation of the output data of the standard control device. If, for example, the input datastream is amended such that the standard control device 4 is told that there is an operating parameter outside the predetermined limits, then the standard control device switches off this bus subscriber, and hence the welding robot, via the bus by means of a safety-related logic linking data item transmitted to that specific bus subscriber 38. In the same way, the safety analyzer can cancel enabling by the standard control device, by overwriting the appropriate output data item.

Fig. 6b shows the situation in which the safety analyzer amends the output datastream on the bus. In this situation, the safety analyzer manipulates the data sent to the bus subscriber 38 such that the bus subscriber switches off its output, and hence the welding robot as well.

Fig. 2 shows a further embodiment of the invention. In this case, the bus is a system operating on the master-slave principle, with the standard control device acting as the master, and the individual bus subscribers acting as slaves. The bus system is connected via an interface assembly 41 to a host 40, with the process-related control system being arranged and running in the host, and the safety-related control system being arranged and running in the interface assembly. The system has a single safety analyzer 5, which is coupled to the bus directly after the interface assembly, in order to monitor the bus datastream. This measure ensures that the safety analyzer can monitor the entire input datastream as well as the entire output datastream on the bus, when connected to a serial bus with a ring structure. The safety analyzer 5 uses the knowledge of the entire datastream via the bus to store the complete process map in a memory provided for this purpose, in the described embodiment. In consequence, the safety analyzer is able to check all the safety-related logic linking data for the safety-related control system in the interface assembly and, if necessary, that is to say when a fault occurs, to drive the output 6 to switch the entire system off by means of the contactor 7 on a safety basis, such that the supply voltage is switched off for the entire system.

The automation system according to the invention in Fig. 3 shows a modification of the embodiment illustrated in Fig. 2. In this case, the safety analyzer 5 is integrated in the interface assembly 41. The safety-related control of the standard control device and the safety-related data processing in the safety analyzer run in separate and independent logic modules in the interface assembly. Furthermore, a second safety analyzer 5'' is arranged at the head of the local bus spur 8. This arrangement is in turn dependent on the safety analyzer 5'' being able to

monitor all the input data and output data for the subscribers 33, 34 and 35 on the local bus spur 8 and, accordingly, of being able to apply a complete process map for the process sequence within the local bus spur. Like the safety analyzer 5 in the  
5 long-distance bus section, the safety analyzer 5'' is thus able to check all the safety-related logic linking data for the safety-related control system for the local bus section in the interface assembly and, if necessary and as described above, to initiate the necessary safety-related functions by data  
10 manipulation. This allows very stringent safety requirements which are placed on the safety-relevant inputs and outputs applicable to the bus spur 8 to be satisfied, since the local bus spur 8 is protected not only by the safety-related control of the standard control device, but also by the safety analyzer 5 and by  
15 the safety analyzer 5''.

Fig. 4 shows a further embodiment of the invention. The automation system according to the invention has two safety analyzers 5 and 5', whose safety-related outputs 6 and 6' are coupled to one another. Both outputs control a multiple contactor  
20 device 7 for switching off the supply voltage for the entire system. The system is controlled via a standard control device 4 via the serial bus 2. Since it is arranged in the system, the safety analyzer 5 can monitor all the input and output data on the bus, except for the input data for the first bus subscriber  
25 31, which is arranged between the control device 4 and the safety analyzer 5. The safety analyzer 5' can monitor all the input data on the bus, but none of the output data except for that for the last bus subscriber is accessible to it. By copying the relevant data in the bus data flow, the first safety analyzer 5 is  
30 therefore able to copy the output data accessible to it into input data and thus to make available to the safety analyzer 5'

as well the output data, which is actually not accessible to said safety analyzer 5', for application of a process map for the safety-related bus subscriber 32 to be protected. Since both safety analyzers receive the same input information, they can  
5 monitor the safety-related inputs and outputs of the bus subscriber 32 to be protected. This provides distributed redundancy for the safety technology in the automation system according to the invention. In the present example, the safety analyzer 5' also has a safety-related input 10, to which an  
10 emergency switch 13 is connected. When the emergency switch 13 is closed, the safety analyzer 5' responds with the associated safety-related function in the safety analyzer, namely the opening of the contactor 7 in order to switch off the entire system.

15 The described method for copying input data into output data, and vice versa, is also used, according to the invention, to provide a data link between two slaves in the automation system operating on the master-slave principle, without the master being required for data transmission. In this case, for  
20 example, a safety analyzer which is associated with one bus subscriber can insert the data item to be transmitted for the bus subscriber into the input datastream, and thus make it available to a downstream bus subscriber, without involving the master. In this way, if required, information can be multicast or broadcast  
25 in a simple manner to all the other downstream bus subscribers.

In one embodiment of the invention, which is not illustrated, the safety analyzer is integrated in an associated safety-based bus subscriber. The safety-based logic links are in this case provided in a logic unit in the bus subscriber, so that  
30 intelligence installed in the bus subscriber can be used for the safety-based logic links. Since the bus subscriber has a bus

interface, this considerably reduces the additional hardware complexity for the safety analyzer.

At least in some cases, the safety-related data is transmitted via the bus using a security protocol for data transmission in the described automation systems according to the invention. Depending on the requirement, this security protocol may include, in addition to the safety data item, the negated safety data item, and an address and/or data protection information in the form of a CRC. This allows errors during data transmission to be identified easily. For this purpose, a safety analyzer which is used in the automation system according to the invention is set up such that it can read the security protocol, and can evaluate it appropriately.

The address of the safety bus subscriber transmitted in the security protocol allows the safety analyzer to adapt the programming, to identify the data set of the subscriber associated with it, and to take account of the change in the bus layout when the bus layout is changed, for example as a result of the component being switched off for safety reasons. In addition, the inclusion of the address in the security protocol allows a storage error caused by a bus fault or a failure in the decentralized unit to be detected.

One particular embodiment of a safety analyzer for use in the automation system according to the invention is shown in Fig. 5. The illustrated safety analyzer 5 has not only four safety-based inputs 10 for detecting safety-based information from photodetectors 11, but also four safety-based outputs 6 for disconnecting the supply voltage from four automation bus components by means of contactors. The various safety-based outputs 6 are in this case driven in response to the logic links being produced in the safety analyzer, in response to the

comparison with safety-based logic links in the standard control system, and/or in response to safety-related input information, via the input 10. In this case, interlock logic is stored in the safety analyzer, governing which safety-based functions are initiated when a specific fault or error occurs, that is to say which components must be disconnected from the supply voltage when that fault or error occurs.

It is within the scope of the invention for a safety analyzer to carry out process data processing in addition to processing safety-related data.

It should furthermore be stated that the principle of the invention is not restricted to the automation bus systems described in the exemplary embodiments but, in fact, can be applied to all automation systems having a bus.

## ENGLISH TRANSLATION OF ANNEXES 107018721

21

531 Rec'd PCT. 14 DEC 2001

Claims

1. An automation system (1), comprising at least  
- a bus system (2),  
5 - I/O bus subscribers (31 - 38) connected to it and  
a standard control device (4; 40, 41), as well as  
- at least one safety analyzer (5, 5', 5'') which  
monitors the data flow via the bus system and is  
designed to carry out at least one safety-related  
10 function,  
characterized in that  
the safety analyzer is set up for checking and  
processing safety-related data in the bus datastream  
and/or has a device for manipulating the datastream  
15 transmitted on the bus (2).
2. The automation system (1) as claimed in claim 1,  
characterized in that  
the standard control device controls at least one  
20 safety-related Output.
3. The automation system (1) as claimed in claim 1 or  
2,  
characterized in that  
25 the safety analyzer (5, 5', 5'') has a freely  
programmable logic device, which processes the monitored  
data, in particular the monitored safety-related data.
4. The automation system (1) as claimed in one of  
30 claims 1 to 3,  
characterized in that  
the safety analyzer (5, 5', 5'') is not a logic bus

6. The automation system as claimed in one of claims 1 to 5,  
characterized in that  
the safety analyzer (5') has at least one safety-related input (10), via which the safety analyzer is connected to a safety-related device (11) in the automation system for detecting safety-related data.

30     8.     The automation system (1) as claimed in one of  
claims 1 to 7,  
characterized in that

the bus (2) is a serial bus, and at least one safety analyzer (5, 5') is arranged in the long-distance bus section of the automation system.

- 5 9. The automation system (1) as claimed in claim 8, characterized in that  
a safety analyzer (5) is arranged directly after the host (40) or after the interface assembly (41).
- 10 10. The automation system (1) as claimed in one of claims 1 to 9, characterized in that  
a safety analyzer (5) is arranged in the interface assembly (41).
- 15 11. The automation system (1) as claimed in one of the preceding claims 1 to 10, characterized in that  
the safety analyzer (5, 5', 5'') comprises a memory device for storing a process map.
- 20 12. The automation system (1) as claimed in one of the preceding claims 1 to 11, characterized in that  
the safety analyzer (5, 5', 5'') has a device for manipulating the input and/or output data transmitted on the bus (2).
- 25 13. The automation system (1) as claimed in claim 12, characterized in that  
the device overwrites input and/or output data in the safety analyzer (5, 5', 5''), and/or inserts data into the datastream.
- 30

14. The automation system (1) as claimed in one of the preceding claims 1 to 13,  
characterized in that  
5 at least one safety analyzer (5, 5', 5'') is of redundant design.
15. A method for operating an automation system, in particular an automation system (1) as claimed in one of  
10 claims 1 to 14,  
characterized in that  
a standard control device (4; 40, 41) carries out a process control with the processing of process-linked I/O data and safety-related control with the processing  
15 of safety-related data, and, furthermore, processing of safety-related data is carried out in at least one safety analyzer (5, 5', 5''), with safety-related data, in particular safety-related logic linking data in the bus datastream, being processed in the safety analyzer.  
20
16. The method as claimed in claim 15,  
characterized in that  
the standard control device controls at least one safety-related output.
- 25
17. The method as claimed in claim 15 or 16,  
characterized in that  
a comparison of the safety-related logic linking data, which is transmitted via the bus, for the standard  
30 control device (4, 41) and/or of at least one further safety analyzer (5, 5', 5'') with the corresponding logic linking data of the first safety analyzer, is carried out in a safety analyzer (5, 5', 5'').

18. The method as claimed in one of claims 15 to 17,  
characterized in that  
the logic linking data, which is produced by the  
5 standard control (4, 41) and is sent as output data via  
the bus, is checked in at least one safety analyzer (5,  
5', 5'') by modeling the safety-related logic links of  
the standard control (4, 41).
- 10 19. The method as claimed in one of claims 15 to 18,  
characterized in that  
safety-related functions are carried out in  
response to the check or the comparison by the safety  
analyzer (5, 5', 5'').
- 15 20. The method as claimed in one of claims 15 to 19,  
characterized in that  
a safety-related function is carried out via a  
safety-related output (6) of the safety analyzer (5, 5',  
20 5'').
21. The method as claimed in one of claims 15 to 20,  
characterized in that  
the safety analyzer carries out safety-related  
25 functions in response to the safety-related data  
detected via the safety-related input (10) of the safety  
analyzer (5').
22. The method as claimed in claim 21,  
30 characterized in that  
the process of carrying out the safety-related  
function comprises switching at least one assembly in  
the automation bus system, in particular a bus

subscriber (32 - 38), on or off.

23. The method as claimed in one of claims 15 to 22,  
characterized in that

5 the safety analyzer (5', 5'') overwrites or deletes  
at least one data item in the datastream and/or inserts  
at least one data item into the bus datastream by means  
of a device for manipulating the datastream an the bus  
(2).

10

24. The method as claimed in claim 23,  
characterized in that

the safety analyzer (5, 5', 5'') at least partially  
stores the monitored datastream and copies input data in  
15 the bus datastreams to output data in the bus  
datastream, and vice versa.

25. The method as claimed in one of claims 15 to 24,  
characterized in that

20 safety-related data is transmitted via the bus (2)  
using a security protocol.

26. The method as claimed in claim 25,  
characterized in that,

25 in addition to the safety data item, the security  
protocol comprises the negated safety data item, a  
sequential number, an address and/or data protection  
information (CRC).

30 27. The method as claimed in one of claims 15 to 26,  
characterized in that  
the bus is a system operating an the master-slave

principle, with data being transmitted between at least two slaves, in particular between individual bus subscribers (31 - 38), by means of a data link via at least one safety analyzer (5 5', 5''), with the safety analyzer copying data in the bus datastream.

28. The method as claimed in one of claims 15 to 27, characterized in that

the bus is a system operating on the master-slave principle, with data being transmitted between at least two slaves, in particular between individual bus subscribers (31 - 38), by means of a data link via the control or the master, with the control or the master copying data in the bus datastream.

29. The method as claimed in one of claims 15 to 28, characterized in that

quality data is produced by means of a safety analyzer (5, 5', 5''), and/or the data which has been read is prepared for further processing.

30. The method as claimed in one of claims 15 to 29, characterized in that

the safety-related logic links used in a safety analyzer (5') are at least partially carried out in redundant form in at least one further safety analyzer (5''), and the same safety functions are at least partially carried out by the two safety analyzers.

31. The method as claimed in one of claims 15 to 30, characterized in that

a safety analyzer also at least partially carries out

29. Nov. 2001 11:37

BLUMBACH KRAMER & PARTNER

ALCOA AG Nr. 3981 S. 52/52

28

process data processing.

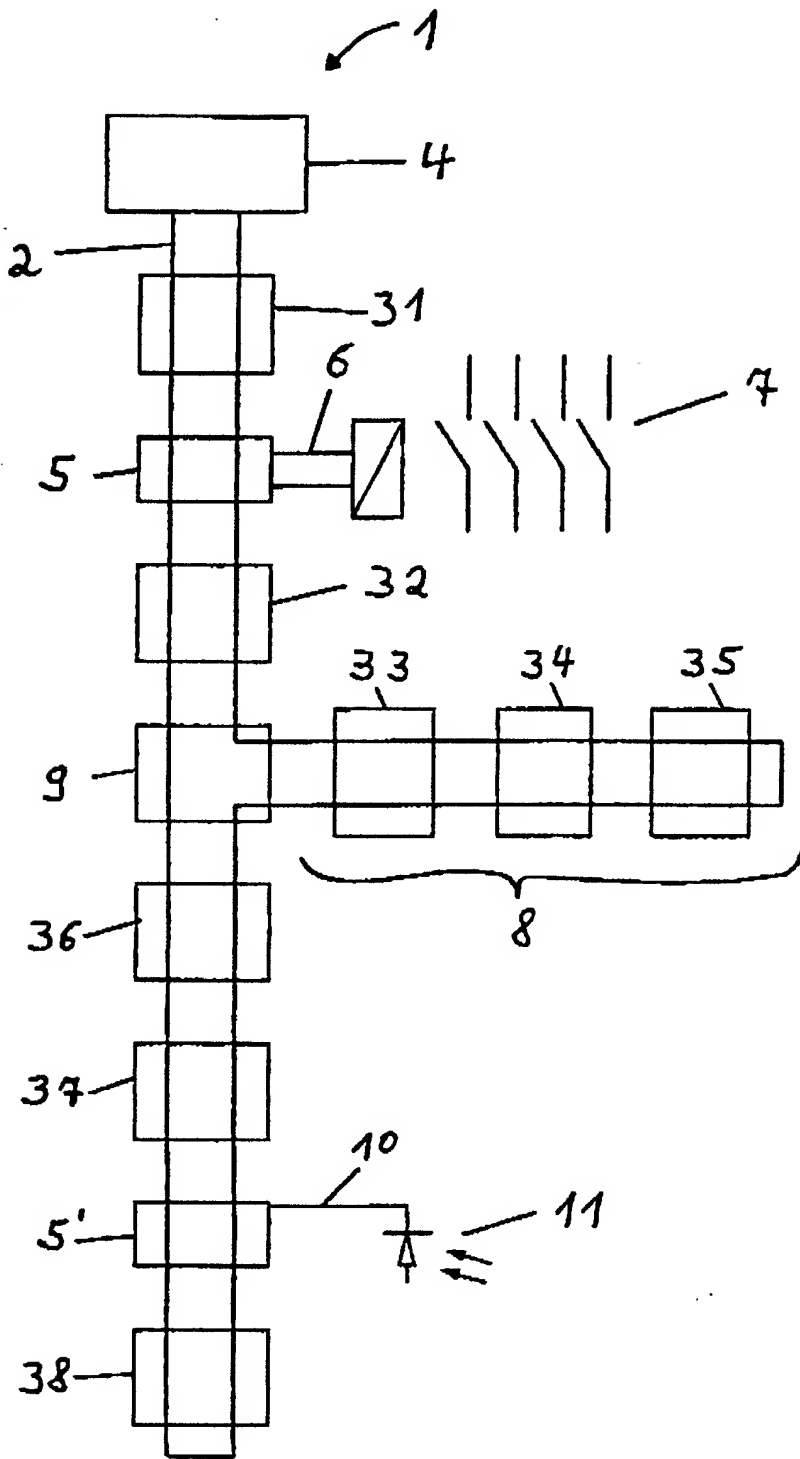


Fig. 1

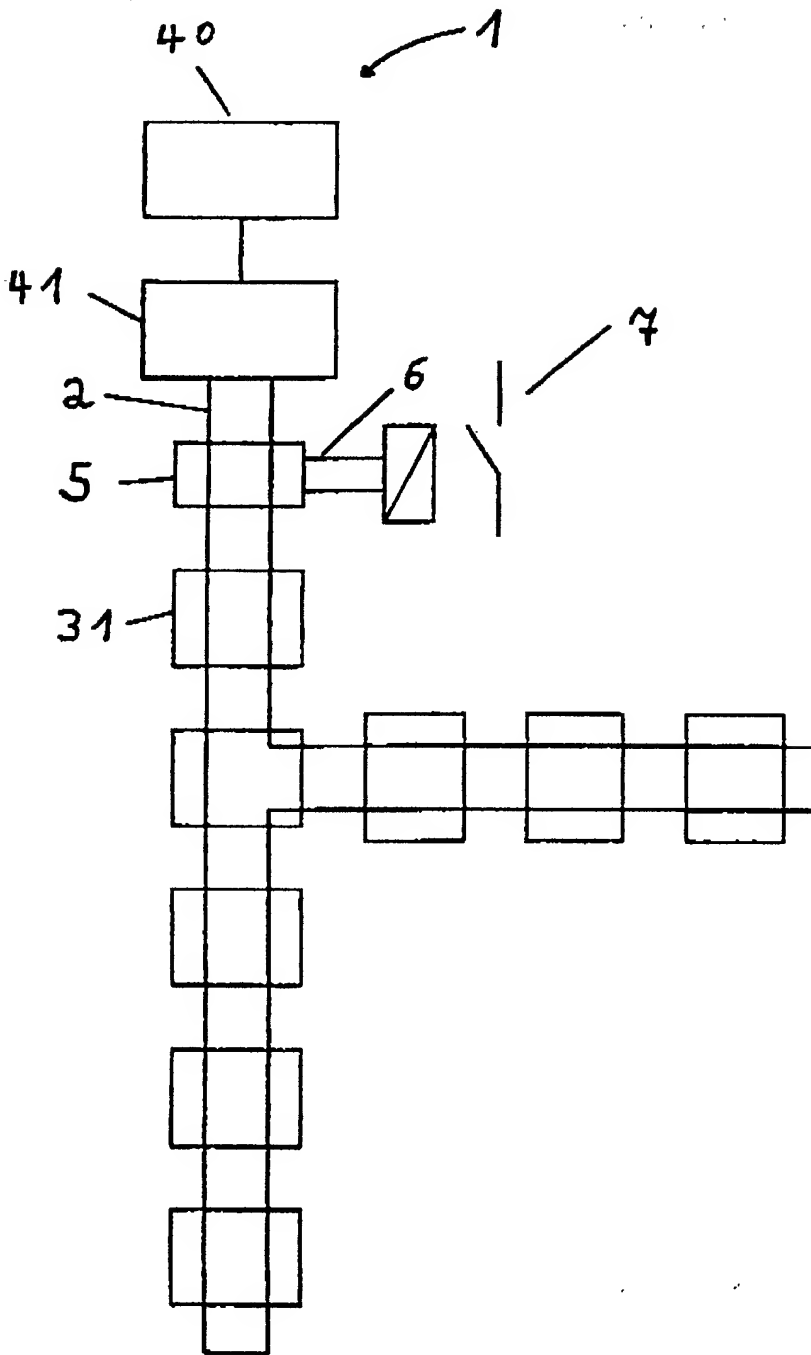


Fig. 2

10/018721

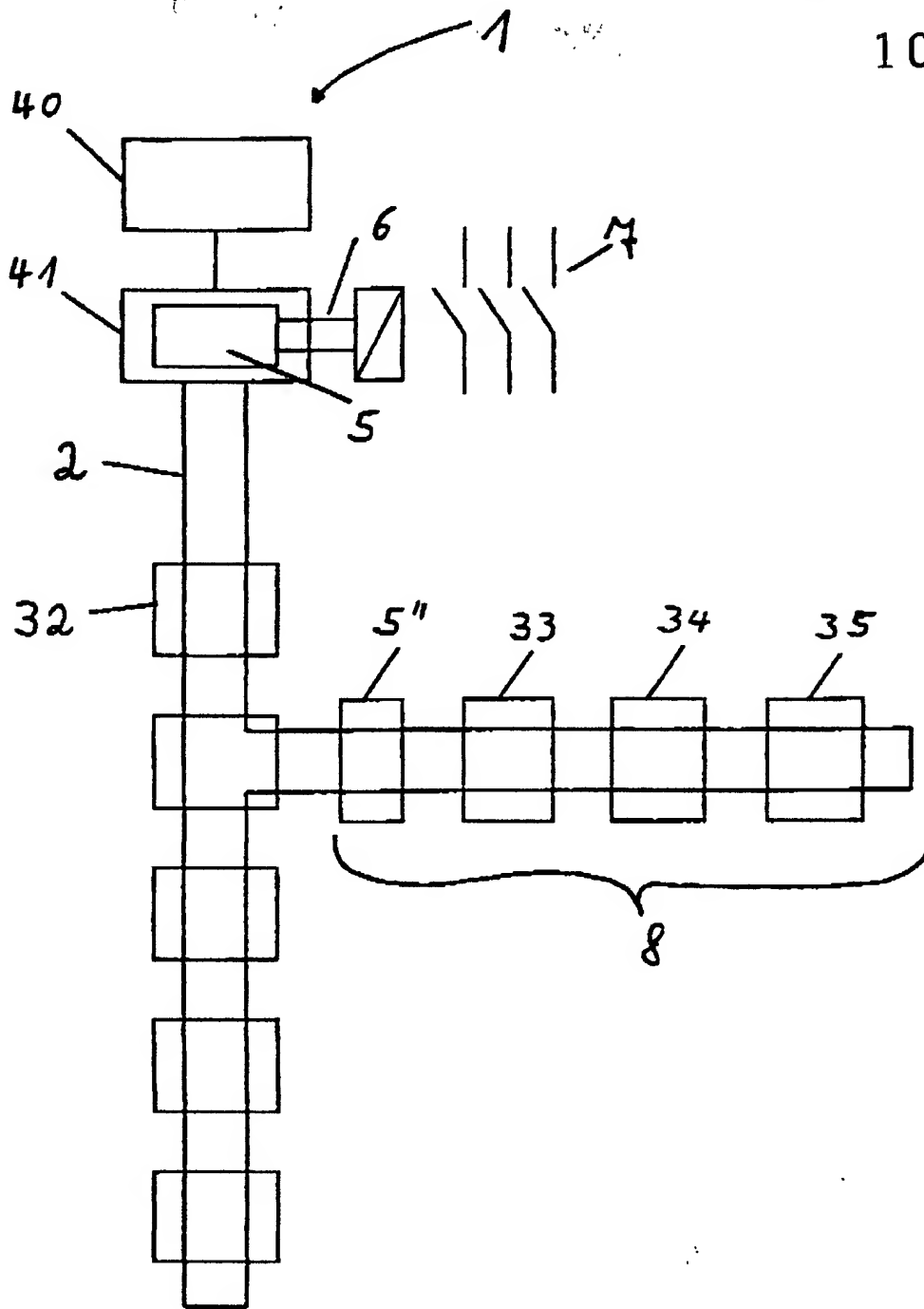


Fig. 3

10/018721

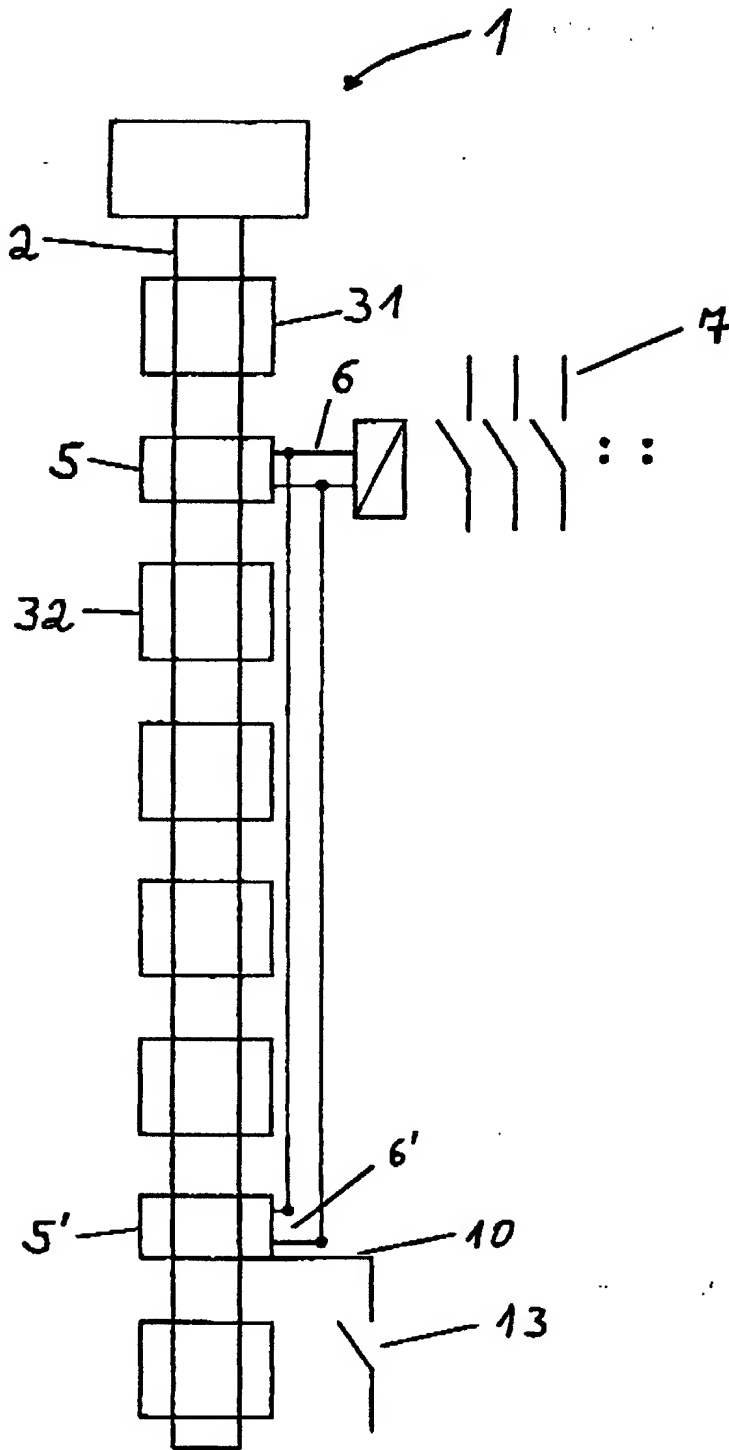


Fig. 4

10/018721

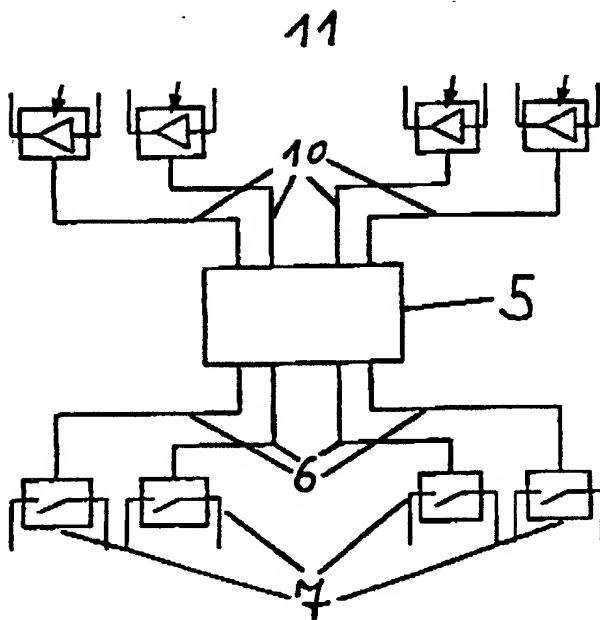


Fig. 5

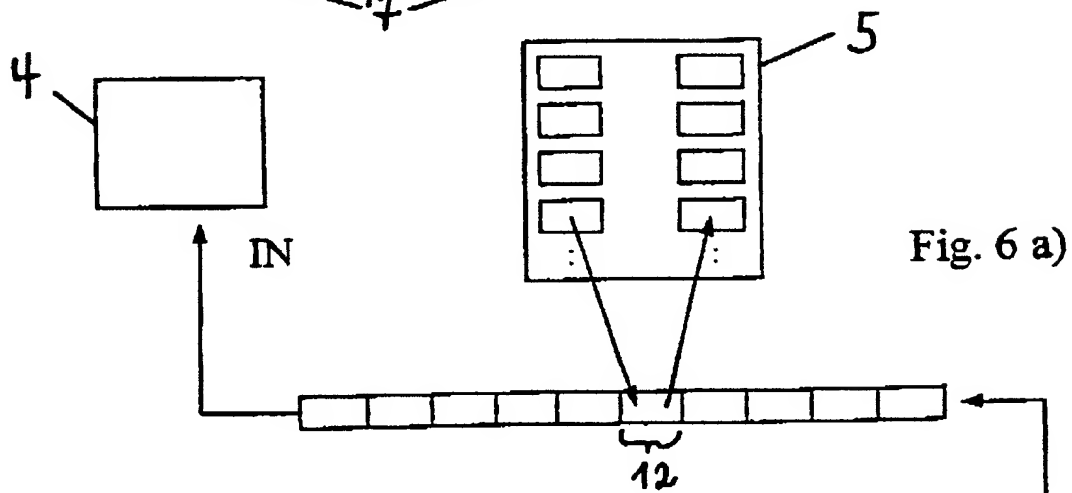


Fig. 6 a)

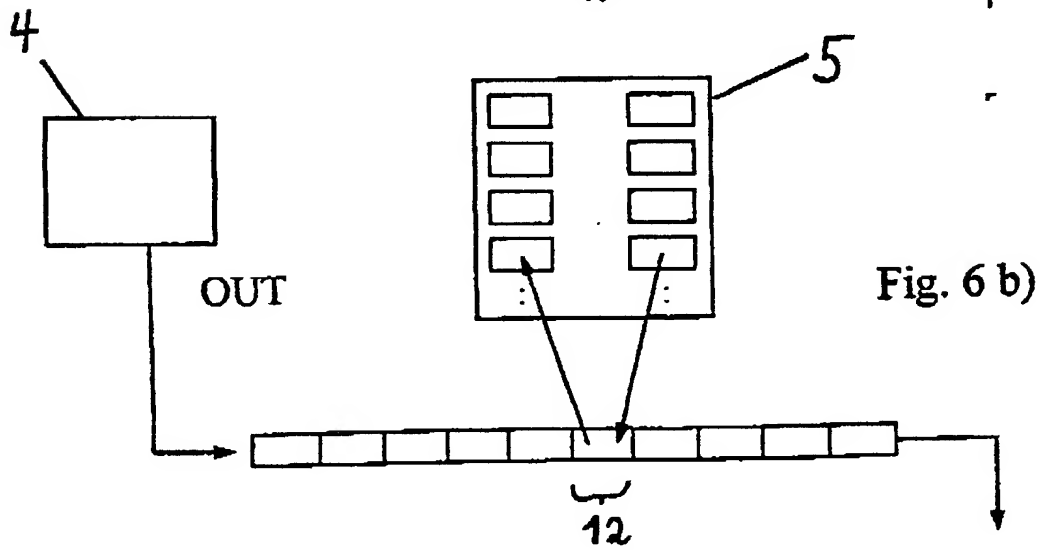


Fig. 6 b)

**Safety-related automation bus system**

**Cross-References to Related Applications**

Not applicable.

**Statement Regarding Federally Sponsored Research or Development**

Not applicable.

**Background of the Invention**

**[0001]** The invention relates to a safety-related automation bus system comprising: at least a bus, I/O bus subscribers connected to the bus, a standard control device, at least one safety analyzer which monitors data flow via the bus system and is designed to carry out at least one safety-related function, and to a method for operation such a system.

**Technical Field**

**[0002]** Control and data transmission systems have gained a dominant position not only in industrial manufacturing owing to the high level of automation that they make possible. Such automation systems generally have at least sections or components in which more stringent requirements with respect to safety may be placed. For example, it is necessary to ensure that certain machines are operated within predetermined operating parameters, or it is necessary to prevent a machine from running even though someone is located in its operating area. In this context, for example, a lathe must not exceed a predetermined rotation speed or there must not be anyone in the radius of action of a robot, when that robot is being operated. Furthermore, when operating an automation system, it is necessary to ensure that, if one component in the system fails, the system does not change to an undefined, and hence unpredictable, state.

**[0003]** On approach to this problem according to the prior art is, in particular, to use a

number of channels for the safety-relevant components in the system, that is to say to design them to be redundant. For example, safety bus components, that is to say for example bus subscribers which are associated with a safety-relevant machine, may be duplicated in an automation bus system. At the same time, the central control and the bus may have a number of channels, or even a specific safety control system, which is separate from the process control system and in some circumstances is of redundant design, for controlling the safety-relevant components. This safety control system essentially carries out the logic links on the safety-related input information and then transmits, for example via an automation bus, safety-related logic linking data to output components. The output components themselves process the received safety measures and, if the test result is positive, output this to the peripherals. Furthermore, they switch their outputs to a safe state if they find a fault, or have no longer received any valid data within a predetermined time period.

**[0004]** The use of two control systems in the system, that is to say a process control system and the described safety control system, results in a number of disadvantages, however. Among other factors, the increasingly stringent requirements for the reaction time of automation systems means that such a system often has to be subdivided between safety islands. Furthermore, synchronization problems occur especially in multichannel control systems which, despite the system in principle being intact, can lead to failures or even to destruction of machine parts. Furthermore, the multichannel design results in an increase in the system and maintenance costs, due to the increased hardware complexity.

**[0005]** DE 198 15 150 A1 discloses a system which comprises an evaluation unit which is connected to the bus, continuously monitors the symbols transmitted via the bus system,

## Summary of the Invention

**[0008]** The invention solves this problem by means of an automation bus system (1) having at least a bus (2), I/O bus subscribers (31-38) connected to the bus (2), a standard control device (4, 40 41), at least one safety analyzer (5, 5', 5'') which monitors data flow via the bus system and is designed to carry out at least one safety-related function, wherein the safety analyzer is at least one of set up for checking and processing safety-related data in a bus datastream and having a device for manipulating the datastream transmitted on the bus (2). The invention solves the above identified problem by a method for operating such a control and data processing system comprising the following steps: using a standard control device (4, 40, 41) for carrying out a process control, with the processing of process-linked I/O data and safety-related data, and, carrying out processing of safety-



**[0010]** A system is therefore provided which can be matched extremely flexibly to the respective requirements for the automation system. For example, each safety bus component may be allocated such a safety analyzer, and a safety analyzer may itself also be integrated in the safety component, for example a safety bus subscriber, although it is also possible for one individual safety analyzer to carry out the processing of safety-related data or the checking of safety-related logic linking data in the bus datastream for a number of safety bus components, or even for all the safety bus components in the system.

**[0011]** The principle of the invention is based in the inventor's experience on the fact that the electronics used in present-day automation systems themselves fail only rarely. The integration of the present-day digital safety technology in automation technology in the form of safety control systems or safety bus systems according to the prior art frequently have the disadvantage of decreasing the system availability. In order to reduce the down times, availability structures are therefore also used in addition to said safety components, but they themselves lead to a not inconsiderable increase in costs, due to the increased hardware complexity.

**[0012]** The invention is therefore based on the reliability of present-day automation systems, and integrates pure emergency electronics or software, which become actively involved in the operation of the system only when the standard technology is operating incorrectly. The standard control device therefore also processes safety-related data, that is to say it controls safety-relevant inputs and outputs. In particular, the safety-related logic linking data which is produced in the bus datastream is, however, monitored and checked by the safety analyzer. This has the advantage for the user that it is no longer absolutely

**[0013]** In order to comply with the relevant safety requirements, the safety analyzer can initiate the necessary safety-related functions in response to the checking and/or the processing of safety-related data, in particular of logic linking data in the bus datastream. In this case, the safety analyzer can react not only to OUT data, that is to say logic linking data from the standard control device, but also to IN data, that is to say to information in the bus datastream, which has been sent from individual I/O bus subscribers to the standard control device.

**[0014]** In order to identify an error in safety-related logic linking data which is transported via the bus, the safety analyzer may have a fully programmable logic device, in which the monitored data, in particular the monitored safety-related data, is processed. In this way, by modeling the safety-related logic links of the standard control system, the safety analyzer can check the logic linking data of this control system sent as OUT data via the bus, and can carry out the necessary safety-related functions in response to the check or

the comparison. In order, for example, to change the system to a safe state, the safety analyzer may have an output via which an assembly in particular a bus subscriber in the automation system, can be switched on or off. The switching-off process can be carried out by disconnection from the voltage supply. In order to change all the associated and mutually independent bus subscribers to a safe state, the safety analyzer may be set up for switching off a bus spur, a safety island comprising a number of mutually associated bus subscribers, or to switch off components on the basis of interlocking logic stored in the analyzer. However, it is also possible for the entire system to be disconnected from the voltage supply via the safety-related output of the safety analyzer.

**[0015]** In addition to monitoring the bus, the safety analyzer can also detect safety-related information via a direct input, by means of which the safety analyzer is connected to a safety-related device in the automation bus system. In this case, this device may be, but need not be, connected to the bus. By way of example, the safety-related information accessible in this way includes the instantaneous rotation speed of the lathe already mentioned, with the analyzer output switching off the machine if a predetermined limiting rotation speed is exceeded.

**[0016]** In order to separate the safety-related information and the process data in the system, and in particular in the control system, the bus system may be connected via an interface assembly to a host, with the process-related control of the standard control device being arranged in the host, and the safety-related control of the standard control device being arranged in the interface assembly. The safety-related control system may, for example, advantageously be in the form of software functional modules, which carry out the necessary logic links on the safety-relevant I/O Information.

**[0017]** The safety-related control system can thus be implemented in the same way as the process control system. When coding the safety-related logic links, the programmer is independent of the programming language being used, in the same way as with the process control system.

**[0018]** The logic links in the safety analyzer have approximately the same scope as the logic links in the host and in the interface assembly, and can be produced either in the same programming language, or else in a different one. The safety analyzer also carries out a comparison of the logic links between the results from the host system and/or the interface assembly and its own results, and starts safety-based functions, for example in the event of an inequality.

**[0019]** The acceptance procedure for such a system can be carried out considerably more easily than is the case with systems according to the prior art. The system can be started up with all the safety interlocks, without needing to switch the safety technology to be active. The necessary logic links are in this case located in the host system or in the interface assembly. The functionality of the system can be investigated first of all using a black-box test. In a second step, the safety technology is then connected, in the form of the safety analyzer or analyzers. Since only the safety logic links, but not the process data logic links, are present there, the white-box test can now be carried out quickly and clearly, thus allowing the acceptance times to be considerably reduced. Since the safety-related logic algorithms can also run on the host system and/or on the interface assembly, a comparison with those in the analyzer can be carried out quickly.

**[0020]** If the bus is a serial ring bus, for example a bus in accordance with EN 50254, and if a safety analyzer is arranged in the top-level long-distance bus section of the automation

system, then this has access to all the IN data in the system since, in the system referred to, the data is carried in a forward transmission line and in a return transmission line by each bus subscriber. The analyzer is thus able to form a process map which is restricted to the IN data and the Out data to which it has access.

**[0021]** In bus systems with a linear topology, the safety analyzer can in general read all the information at any point in the bus system, and can thus produce a complete process map.

**[0022]** In one advantageous embodiment of the invention, the safety analyzer is arranged in a serial ring bus system directly after the host or the interface assembly, so that it can form a complete process map. The safety analyzer is thus able to check and to process safety-based data, in particular safety-based logic linking data, for its correctness at any time and fully, since, in this case, the analyzer has access to all the In and Out data, that is to say all the input and output data.

**[0023]** If the safety analyzer is arranged in the interface assembly of the described serial ring bus system, then the function of the safety analyzer can be carried out by means of a software component in the interface assembly. The interface assembly in this case advantageously has a safety-related output, in order to carry out appropriate safety-based functions, for example using a contactor to switch off a supply voltage.

**[0024]** However, in one particular advantageous embodiment of the invention, such safety-based functions can be carried out by direct data manipulation of the bus datastream by means of the safety analyzer. The manipulation includes rewriting, adding, insertion or substitution both of OUT data and of IN data in the bus datastream. If the process map is known, the safety analyzer can thus influence the operation of the automation system according to the invention in a far-reaching form, and can thus ensure that the system can

be kept in defined states at any time. The principle of data manipulation can furthermore also be used in order to make available bus datastream components which are generally not accessible in a safety analyzer arranged in the bus spur, in that a safety analyzer which is arranged in the long-distance bus converts the relevant data to data which is transported in the relevant bus spur. This provides a direct data link between safety analyzers.

**[0025]** Data manipulation by means of a safety analyzer can also be used, in a bus system operating on the master-slave principle, in order to transmit data between at least two slaves, in particular between individual bus subscribers, by means of a point-to-point link via at least one safety analyzer, with the safety analyzer copying data in the bus datastream. Depending on the position of the two slaves in the bus system, the master is in some circumstances not included in this data link, so that the data transportation takes place completely independently of the bus master. Such a data link between two slaves is, apart from this, also possible when the bus master is carrying out a copying function. While, when a safety analyzer is acting as an agent, as described above, the bus master is not included in the data transportation, at least in certain situations, the bus master is absolutely essential for the second form of point-to-point link between two slaves.

**[0026]** The interchanging of data between at least two slaves, for example between individual bus subscribers, by means of a point-to-point link can, furthermore, also be provided by including the master or the control system in the transmission, with the master or the control system in this case copying the data in the bus datastream.

**[0027]** In order to improve the data security, the safety-related data can also be transmitted via the bus using a security protocol. For example, the security protocol may include not only the safety data item but also the negated safety data item, a sequential number, an





linking data to safety-related outputs. By way of example, the standard control device may send a switch-off command for said lathe via the bus to the associated bus subscriber 32 when the maximum rotation speed has been exceeded and there is thus a risk of the system running out of control. In this case as well, the safety-related controller in the standard control device communicates via the bus with the safety-related output.

**[0037]** The automation system according to the invention also has two safety analyzers 5, 5', each of which monitors the data flow via the bus system in real time by means of an interface. The safety analyzers are set for logic linking and/or processing of safety-related data in the bus datastream. This means that they can deal with the safety-related logic links of the standard control device, since they can access the safety-related data transported via the bus.

**[0038]** To this end, the safety analyzers 5, 5' each have a freely programmable logic device in which the monitored data, in particular the monitored safety-related data, is processed. By way of example, the safety analyzers 5, 5' can model the safety-related logic links of the standard control system to check their logic linking data sent via the bus as output data. In the present case, the safety-related logic links relate to an individual bus subscriber 32. In this case, the safety analyzer 5 is responsible for the safety-related inputs and outputs which are associated with this bus subscriber. In the embodiment of the invention illustrated in Fig. 1, the safety analyzers 5 and 5' are not logical bus subscribers in the automation system. However, the safety analyzer 5 has a safety-related output 6 via which the bus subscriber 32 associated with the safety analyzer can be switched off. This is done by means of a circuit of a contactor 7, which disconnects the bus subscriber and the connected assemblies and machines from the supply voltage. In this way, the safety

analyzer 5 carries out a safety-related function in response to the check or the comparison, in this case switching off the supply voltage. If, for example, a fault is identified in the safety-related logic linking data from the standard control device, the safety analyzer can switch off the relevant bus subscriber via the described output, since the safety-related controller provided by the standard control device is no longer operating correctly. In a similar way, a bus subscriber is switched off if the safety-related controller does not send the required data to that bus subscriber and, in consequence, there is a risk of the system changing to an undefined state.

**[0039]** In the described embodiment, a local bus spur 8 with three bus subscribers 33, 34 and 35 is arranged via a bus coupler 9. These bus subscribers are dependent on the functionality and on the operation of the bus subscriber 32, which is associated with the safety analyzer 5. It is therefore necessary, when the bus subscriber 32 is switched off, for the bus subscribers on the local bus spur 8 to be disconnected from the supply voltage, as well. This interlocking logic is stored in the safety analyzer 5. A total of four bus subscribers must therefore be switched off, together with their subordinate assemblies and machines, as is illustrated schematically in Fig. 1 by means of a quadruple contactor 7.

**[0040]** The safety analyzer 5', like the first safety analyzer 5, is set up for monitoring the data transported via the bus. However, in contrast to the first safety analyzer 5, it does not have an input by means of which it can carry out safety-related functions. Instead of this, it has a safety-related input 10, via which the safety analyzer is connected to a safety-related device 11 in the automation system for detecting safety-related data. In the present case, this device 11 has a photodetector which, as part of a light barrier monitors the operating area of a welding robot. The sensor is not connected to the automation bus by

Meyer-Gräfe  
(H) 01PH0419USP  
PCT/DE00/01901

subscriber 38 such that the bus subscriber switches off its output, and hence the welding robot as well.

**[0042]** Fig. 2 shows a further embodiment of the invention. In this case, the bus is a system operating on the master-slave principle, with the standard control device acting as the master, and the individual bus subscribers acting as slaves. The bus system is connected via an interface assembly 41 to a host 40, with the process-related control system being arranged and running in the host, and the safety-related control system being arranged and running in the interface assembly. The system has a single safety analyzer 5, which is coupled to the bus directly after the interface assembly, in order to monitor the bus datastream. This measure ensures that the safety analyzer can monitor the entire input datastream as well as the entire output datastream on the bus, when connected to a serial bus with a ring structure. The safety analyzer 5 uses the knowledge of the entire datastream via the bus to store the complete process map in a memory provided for this purpose, in the described embodiment. In consequence, the safety analyzer is able to check all the safety-related logic linking data for the safety-related control system in the interface assembly and, if necessary, that is to say when a fault occurs, to drive the output 6 to switch the entire system off by means of the contactor 7 on a safety basis, such that the supply voltage is switched off for the entire system.

**[0043]** The automation system according to the invention in Fig. 3 shows a modification of the embodiment illustrated in Fig. 2. In this case, the safety analyzer 5 is integrated in the interface assembly 41. The safety-related control of the standard control device and the safety-related data processing in the safety analyzer run in separate and independent logic modules in the interface assembly. Furthermore, a second safety analyzer 5'' is arranged

at the head of the local bus spur 8. This arrangement is in turn dependent on the safety analyzer 5'' being able to monitor all the input data and output data for the subscribers 33, 34 and 35 on the local bus spur 8 and, accordingly, of being able to apply a complete process map for the process sequence within the local bus spur. Like the safety analyzer 5 in the long-distance bus section, the safety analyzer 5'' is thus able to check all the safety-related logic linking data for the safety-related control system for the local bus section in the interface assembly and, if necessary and as described above, to initiate the necessary safety-related functions by data manipulation. This allows very stringent safety requirements which are placed on the safety-relevant inputs and outputs applicable to the bus spur 8 to be satisfied, since the local bus spur 8 is protected not only by the safety-related control of the standard control device, but also by the safety analyzer 5 and by the safety analyzer 5''.

**[0044]** Fig. 4 shows a further embodiment of the invention. The automation system according to the invention has two safety analyzers 5 and 5', whose safety-related outputs 6 and 6' are coupled to one another. Both outputs control a multiple contactor device 7 for switching off the supply voltage for the entire system. The system is controlled via a standard control device 4 via the serial bus 2. Since it is arranged in the system, the safety analyzer 5 can monitor all the input and output data on the bus, except for the input data for the first bus subscriber 31, which is arranged between the control device 4 and the safety analyzer 5. The safety analyzer 5' can monitor all the input data on the bus, but none of the output data except for that for the last bus subscriber is accessible to it. By copying the relevant data in the bus data flow, the first safety analyzer 5 is therefore able to copy the output data accessible to it into input data and thus to make available to the

**[10045]** The described method for copying input data into output data, and vice versa, is also used, according to the invention, to provide a data link between two slaves in the automation system operating on the master-slave principle, without the master being required for data transmission. In this case, for example, a safety analyzer which is associated with one bus subscriber can insert the data item to be transmitted for the bus subscriber into the input datastream, and thus make it available to a downstream bus subscriber, without involving the master. In this way, if required, information can be multicast or broadcast in a simple manner to all the other downstream bus subscribers.

**[0046]** In one embodiment of the invention, which is not illustrated, the safety analyzer is integrated in an associated safety-based bus subscriber. The safety-based logic links are in this case provided in a logic unit in the bus subscriber, so that intelligence installed in the bus subscriber can be used for the safety-based logic links. Since the bus subscriber has a bus interface, this considerably reduces the additional hardware complexity for the safety

analyzer.

**[0047]** At least in some cases, the safety-related data is transmitted via the bus using a security protocol for data transmission in the described automation systems according to the invention. Depending on the requirement, this security protocol may include, in addition to the safety data item, the negated safety data item, and an address and/or data protection information in the form of a CRC. This allows errors during data transmission to be identified easily. For this purpose, a safety analyzer which is used in the automation system according to the invention is set up such that it can read the security protocol, and can evaluate it appropriately.

**[0048]** The address of the safety bus subscriber transmitted in the security protocol allows the safety analyzer to adapt the programming, to identify the data set of the subscriber associated with it, and to take account of the change in the bus layout when the bus layout is changed, for example as a result of the component being switched off for safety reasons. In addition, the inclusion of the address in the security protocol allows a storage error caused by a bus fault or a failure in the decentralized unit to be detected.

**[0049]** One particular embodiment of a safety analyzer for use in the automation system according to the invention is shown in Fig. 5. The illustrated safety analyzer 5 has not only four safety-based inputs 10 for detecting safety-based information from photodetectors 11, but also four safety-based outputs 6 for disconnecting the supply voltage from four automation bus components by means of contactors. The various safety-based outputs 6 are in this case driven in response to the logic links being produced in the safety analyzer, in response to the comparison with safety-based logic links in the standard control system, and/or in response to safety-related input information, via the

input 10. In this case, interlock logic is stored in the safety analyzer, governing which safety-based functions are initiated when a specific fault or error occurs, that is to say which components must be disconnected from the supply voltage when that fault or error occurs.

**[0050]** It is within the scope of the invention for a safety analyzer to carry out process data processing in addition to processing safety-related data.

**[0051]** It should furthermore be stated that the principle of the invention is not restricted to the automation bus systems described in the exemplary embodiments but, in fact, can be applied to all automation systems having a bus.



4/PRTS

10013721 1142202

10/018721

531 Rec'd PCT 14 DEC 2001

**“Version with Markings to show Changes Made”**

**Safety-related automation bus system**

Cross-References to Related Applications

Not applicable.

Statement Regarding Federally Sponsored Research or Development

Not applicable.

Background of the Invention

[0001] The invention relates to a safety-related automation bus system [as claimed in the precharacterizing clause of claim 1] comprising: at least a bus, I/O bus subscribers connected to the bus, a standard control device, at least one safety analyzer which monitors data flow via the bus system and is designed to carry out at least one safety-related function, and to a method for operation such a system.

Technical Field

[0002] Control and data transmission systems have gained a dominant position not only in industrial manufacturing owing to the high level of automation that they make possible. Such automation systems generally have at least sections or components in which more stringent requirements with respect to safety may be placed. For example, it is necessary to ensure that certain machines are operated within predetermined operating parameters, or it is necessary to prevent a machine from running even though someone is located in its operating area. In this context, for example, a lathe must not exceed a predetermined rotation speed or there must not be anyone in the radius of action of a robot, when that robot is being operated. Furthermore, when operating an automation system, it is necessary to ensure that, if one component in the system fails, the system does not change

**[0003]** On approach to this problem according to the prior art is, in particular, to use a number of channels for the safety-relevant components in the system, that is to say to design them to be redundant. For example, safety bus components, that is to say for example bus subscribers which are associated with a safety-relevant machine, may be duplicated in an automation bus system. At the same time, the central control and the bus may have a number of channels, or even a specific safety control system, which is separate from the process control system and in some circumstances is of redundant design, for controlling the safety-relevant components. This safety control system essentially carries out the logic links on the safety-related input information and then transmits, for example via an automation bus, safety-related logic linking data to output components. The output components themselves process the received safety measures and, if the test result is positive, output this to the peripherals. Furthermore, they switch their outputs to a safe state if they find a fault, or have no longer received any valid data within a predetermined time period.

**[0004]** The use of two control systems in the system, that is to say a process control system and the described safety control system, results in a number of disadvantages, however. Among other factors, the increasingly stringent requirements for the reaction time of automation systems means that such a system often has to be subdivided between safety islands. Furthermore, synchronization problems occur especially in multichannel control systems which, despite the system in principle being intact, can lead to failures or even to destruction of machine parts. Furthermore, the multichannel design results in an increase in the system and maintenance costs, due to the increased hardware complexity.

[0005] DE 198 15 150 A1 discloses a system which comprises an evaluation unit which is connected to the bus, continuously monitors the symbols transmitted via the bus system, and starts up a piece of equipment only when codings which are transmitted via the bus system are identified without any errors. To this end, the input data sent by the bus subscriber to the master is evaluated, and the piece of equipment is switched on or off in response to the evaluation.

[0006] Such an approach is not as costly as the system described first, but it is highly inflexible in terms of upgrading the system or matching the system to other bus components. Furthermore, the evaluation unit has sole responsibility for initiating a safety-based function, so that it is absolutely essential for the evaluation unit to be of redundant design in order to comply with stringent safety requirements.

#### Summary of the Invention

[0007] One object of the invention is thus to provide a safety-related automation bus system which requires as little hardware redundancy as possible, and which can be flexibly matched to the respective requirements.

[0008] The invention solves this problem by means of an automation bus system [having the features of claim 1 and] (1) having at least a bus (2), I/O bus subscribers (31-38) connected to the bus (2), a standard control device (4, 40 41), at least one safety analyzer (5, 5', 5'') which monitors data flow via the bus system and is designed to carry out at least one safety-related function, wherein the safety analyzer is at least one of set up for checking and processing safety-related data in a bus datastream and having a device for manipulating the datastream transmitted on the bus (2). The invention solves the above identified problem by a method for operating such a control and data processing system

[as claimed in claim 14.] comprising the following steps: using a standard control device (4, 40, 41) for carrying out a process control, with the processing of process-linked I/O data and safety-related data, and, carrying out processing of safety-related data in at least one safety analyzer (5, 5', 5''), with safety-related logic linking data in the bus datastream being processed in the safety analyzer. [Developments of the invention are specified in the dependent claims.]

**[0009]** According to the invention, the automation system comprises a bus system, sensor and actuator bus subscribers connected to it, and a standard control device which carries out the process control function with the processing of process-linked I/O data and safety-related control function with the processing of safety-related data, that is to say the control of safety-related inputs and outputs. It also includes what is referred to as a safety analyzer, which is connected to the bus by means of an appropriate interface and monitors the data flow via the bus, with the analyzer being set up to carry out safety-related functions. This relates, for example, to the actuation of a contractor for switching off the supply voltage to system components, or to the determination of the quality data. Such quality data may include general system parameters, for example data on the occurrence of faults in system components, or bus transmission errors. The automation system is distinguished by the fact that the standard control device drives at least one safety-related output via the bus, but it may itself have such a safety-related output. According to the invention, a safety-related output denotes a sink for safety information which starts safety-based sequences as a function of the information, for example slowing down a machine or even switching off a machine by interrupting the supply power. The safety analyzer in the automation system according to the invention is designed for checking

**[0011]** The principle of the invention is based in the inventor's experience on the fact that the electronics used in present-day automation systems themselves fail only rarely. The integration of the present-day digital safety technology in automation technology in the form of safety control systems or safety bus systems according to the prior art frequently have the disadvantage of decreasing the system availability. In order to reduce the down times, availability structures are therefore also used in addition to said safety components, but they themselves lead to a not inconsiderable increase in costs, due to the increased hardware complexity.

Meyer-Gräfe  
(H) 01PH0419USP  
PCT/DE00/01901

**[0013]** In order to comply with the relevant safety requirements, the safety analyzer can initiate the necessary safety-related functions in response to the checking and/or the processing of safety-related data, in particular of logic linking data in the bus datastream. In this case, the safety analyzer can react not only to OUT data, that is to say logic linking data from the standard control device, but also to IN data, that is to say information in the bus datastream, which has been sent from individual I/O bus subscribers to the standard control device.

**[0014]** In order to identify an error in safety-related logic linking data which is transported via the bus, the safety analyzer may have a fully programmable logic device, in which the

monitored data, in particular the monitored safety-related data, is processed. In this way, by modeling the safety-related logic links of the standard control system, the safety analyzer can check the logic linking data of this control system sent as OUT data via the bus, and can carry out the necessary safety-related functions in response to the check or the comparison. In order, for example, to change the system to a safe state, the safety analyzer may have an output via which an assembly in particular a bus subscriber in the automation system, can be switched on or off. The switching-off process can be carried out by disconnection from the voltage supply. In order to change all the associated and mutually independent bus subscribers to a safe state, the safety analyzer may be set up for switching off a bus spur, a safety island comprising a number of mutually associated bus subscribers, or to switch off components on the basis of interlocking logic stored in the analyzer. However, it is also possible for the entire system to be disconnected from the voltage supply via the safety-related output of the safety analyzer.

**[0015]** In addition to monitoring the bus, the safety analyzer can also detect safety-related information via a direct input, by means of which the safety analyzer is connected to a safety-related device in the automation bus system. In this case, this device may be, but need not be, connected to the bus. By way of example, the safety-related information accessible in this way includes the instantaneous rotation speed of the lathe already mentioned, with the analyzer output switching off the machine if a predetermined limiting rotation speed is exceeded.

**[0016]** In order to separate the safety-related information and the process data in the system, and in particular in the control system, the bus system may be connected via an interface assembly to a host, with the process-related control of the standard control device being

arranged in the host, and the safety-related control of the standard control device being arranged in the interface assembly. The safety-related control system may, for example, advantageously be in the form of software functional modules, which carry out the necessary logic links on the safety-relevant I/O Information.

**[0017]** The safety-related control system can thus be implemented in the same way as the process control system. When coding the safety-related logic links, the programmer is independent of the programming language being used, in the same way as with the process control system.

**[0018]** The logic links in the safety analyzer have approximately the same scope as the logic links in the host and in the interface assembly, and can be produced either in the same programming language, or else in a different one. The safety analyzer also carries out a comparison of the logic links between the results from the host system and/or the interface assembly and its own results, and starts safety-based functions, for example in the event of an inequality.

**[0019]** The acceptance procedure for such a system can be carried out considerably more easily than is the case with systems according to the prior art. The system can be started up with all the safety interlocks, without needing to switch the safety technology to be active. The necessary logic links are in this case located in the host system or in the interface assembly. The functionality of the system can be investigated first of all using a black-box test. In a second step, the safety technology is then connected, in the form of the safety analyzer or analyzers. Since only the safety logic links, but not the process data logic links, are present there, the white-box test can now be carried out quickly and clearly, thus allowing the acceptance times to be considerably reduced. Since the safety-

related logic algorithms can also run on the host system and/or on the interface assembly, a comparison with those in the analyzer can be carried out quickly.

**[0020]** If the bus is a serial ring bus, for example a bus in accordance with EN 50254, and if a safety analyzer is arranged in the top-level long-distance bus section of the automation system, then this has access to all the IN data in the system since, in the system referred to, the data is carried in a forward transmission line and in a return transmission line by each bus subscriber. The analyzer is thus able to form a process map which is restricted to the IN data and the Out data to which it has access.

**[0021]** In bus systems with a linear topology, the safety analyzer can in general read all the information at any point in the bus system, and can thus produce a complete process map.

**[0022]** In one advantageous embodiment of the invention, the safety analyzer is arranged in a serial ring bus system directly after the host or the interface assembly, so that it can form a complete process map. The safety analyzer is thus able to check and to process safety-based data, in particular safety-based logic linking data, for its correctness at any time and fully, since, in this case, the analyzer has access to all the In and Out data, that is to say all the input and output data.

**[0023]** If the safety analyzer is arranged in the interface assembly of the described serial ring bus system, then the function of the safety analyzer can be carried out by means of a software component in the interface assembly. The interface assembly in this case advantageously has a safety-related output, in order to carry out appropriate safety-based functions, for example using a contactor to switch off a supply voltage.

**[0024]** However, in one particular advantageous embodiment of the invention, such safety-based functions can be carried out by direct data manipulation of the bus datastream by

**[0025]** Data manipulation by means of a safety analyzer can also be used, in a bus system operating on the master-slave principle, in order to transmit data between at least two slaves, in particular between individual bus subscribers, by means of a point-to-point link via at least one safety analyzer, with the safety analyzer copying data in the bus datastream. Depending on the position of the two slaves in the bus system, the master is in some circumstances not included in this data link, so that the data transportation takes place completely independently of the bus master. Such a data link between two slaves is, apart from this, also possible when the bus master is carrying out a copying function. While, when a safety analyzer is acting as an agent, as described above, the bus master is not included in the data transportation, at least in certain situations, the bus master is absolutely essential for the second form of point-to-point link between two slaves.

**[0026]** The interchanging of data between at least two slaves, for example between individual bus subscribers, by means of a point-to-point link can, furthermore, also be provided by including the master or the control system in the transmission, with the master or the



second safety analyzer at the head of a bus spur,

[0033] Fig. 4 shows an automation system according to the invention with two safety analyzers whose outputs are connected to one another,

[0034] Fig. 5 shows an outline block diagram illustration of a safety analyzer with various inputs and outputs, and

[0035] Figs. 6a and 6 show an outline illustration of data manipulation on the bus datastream by means of the safety analyzer.

### Detailed Description of the Invention

[0036] Fig. 1 shows an outline illustration of the automation system 1 according to the invention, that is to say a control and data transmission system according to the invention. This has a bus 2 to which I/O bus subscribers with associated sensors and actuators are connected. A standard control device 4 uses the bus for process control, processing process-linked I/O data. To do this, the controller 4 receives data from the individual bus subscribers 31 - 38, which in turn themselves receive data from the standard control device. Furthermore, the standard control device deals with the processing of safety-related data. In this sense, the standard control device carries out not only the process-linked inputs and outputs but also the processing of the safety-relevant inputs and outputs. According to the invention, a safety-related input denotes an information source, with the information emitted by the source being related to some way to the safety of the automation system according to the invention. By way of example, one such safety-related input is the rotation speed sensor of a lathe which is connected to the bus 2 via a bus subscriber 32, since the machine must not rotate at a speed above a predetermined limit. A further example of a safety-related input in the described embodiment of the

invention is a photodetector of a light barrier, which is used to monitor the operating area of the lathe. In this case as well, the standard control device has access via the bus to the information at the safety-related input. After processing the safety-related data, for example in the form of a logic link, the control device 4 sends this safety-related logic linking data to safety-related outputs. By way of example, the standard control device may send a switch-off command for said lathe via the bus to the associated bus subscriber 32 when the maximum rotation speed has been exceeded and there is thus a risk of the system running out of control. In this case as well, the safety-related controller in the standard control device communicates via the bus with the safety-related output.

**[0037]** The automation system according to the invention also has two safety analyzers 5, 5', each of which monitors the data flow via the bus system in real time by means of an interface. The safety analyzers are set for logic linking and/or processing of safety-related data in the bus datastream. This means that they can deal with the safety-related logic links of the standard control device, since they can access the safety-related data transported via the bus.

**[0038]** To this end, the safety analyzers 5, 5' each have a freely programmable logic device in which the monitored data, in particular the monitored safety-related data, is processed. By way of example, the safety analyzers 5, 5' can model the safety-related logic links of the standard control system to check their logic linking data sent via the bus as output data. In the present case, the safety-related logic links relate to an individual bus subscriber 32. In this case, the safety analyzer 5 is responsible for the safety-related inputs and outputs which are associated with this bus subscriber. In the embodiment of the invention illustrated in Fig. 1, the safety analyzers 5 and 5' are not logical bus subscribers in the

automation system. However, the safety analyzer 5 has a safety-related output 6 via which the bus subscriber 32 associated with the safety analyzer can be switched off. This is done by means of a circuit of a contactor 7, which disconnects the bus subscriber and the connected assemblies and machines from the supply voltage. In this way, the safety analyzer 5 carries out a safety-related function in response to the check or the comparison, in this case switching off the supply voltage. If, for example, a fault is identified in the safety-related logic linking data from the standard control device, the safety analyzer can switch off the relevant bus subscriber via the described output, since the safety-related controller provided by the standard control device is no longer operating correctly. In a similar way, a bus subscriber is switched off if the safety-related controller does not send the required data to that bus subscriber and, in consequence, there is a risk of the system changing to an undefined state.

**[0039]** In the described embodiment, a local bus spur 8 with three bus subscribers 33, 34 and 35 is arranged via a bus coupler 9. These bus subscribers are dependent on the functionality and on the operation of the bus subscriber 32, which is associated with the safety analyzer 5. It is therefore necessary, when the bus subscriber 32 is switched off, for the bus subscribers on the local bus spur 8 to be disconnected from the supply voltage, as well. This interlocking logic is stored in the safety analyzer 5. A total of four bus subscribers must therefore be switched off, together with their subordinate assemblies and machines, as is illustrated schematically in Fig. 1 by means of a quadruple contactor 7.

**[0040]** The safety analyzer 5', like the first safety analyzer 5, is set up for monitoring the data transported via the bus. However, in contrast to the first safety analyzer 5, it does not have an input by means of which it can carry out safety-related functions. Instead of this,

it has a safety-related input 10, via which the safety analyzer is connected to a safety-related device 11 in the automation system for detecting safety-related data. In the present case, this device 11 has a photodetector which, as part of a light barrier monitors the operating area of a welding robot. The sensor is not connected to the automation bus by means of a bus subscriber, but is connected directly to the safety analyzer 5'. In response to the safety-related data detected via the safety-related input 10 of the safety analyzer 5', the safety analyzer in this case also carries out a safety-related function. If the photodetector 11 detects that someone has entered the operating area of the robot, then the safety analyzer 5' automatically switches off the corresponding bus subscriber 38 and its associated assemblies, and the robot. To do this, the safety analyzer 5' has a device for manipulating the input and output data transmitted to the bus. In this case, at least one data item in the datastream can be overwritten, deleted and/or at least one data item can be inserted into the bus datastream. Such a procedure is shown in Figs. 6a and 6. These Figs. show the amendment of input and output data for the standard control device 4 by the safety analyzer 5'. In both cases, an information unit 12 is read to a memory in the safety analyzer, and an information unit taken from another memory in the safety analyzer is then written to the corresponding point in the datastream. The bus subscriber and the assemblies connected to it, and hence the robot, can be switched off both via the manipulation of the input data and via the manipulation of the output data of the standard control device. If, for example, the input datastream is amended such that the standard control device 4 is told that there is an operating parameter outside the predetermined limits, then the standard control device switches off this bus subscriber, and hence the welding robot, via the bus by means of a safety-related logic linking data item transmitted

to that specific bus subscriber 38. In the same way, the safety analyzer can cancel enabling by the standard control device, by overwriting the appropriate output data item.

**[0041]** Fig. 6b shows the situation in which the safety analyzer amends the output datastream on the bus. In this situation, the safety analyzer manipulates the data sent to the bus subscriber 38 such that the bus subscriber switches off its output, and hence the welding robot as well.

**[0042]** Fig. 2 shows a further embodiment of the invention. In this case, the bus is a system operating on the master-slave principle, with the standard control device acting as the master, and the individual bus subscribers acting as slaves. The bus system is connected via an interface assembly 41 to a host 40, with the process-related control system being arranged and running in the host, and the safety-related control system being arranged and running in the interface assembly. The system has a single safety analyzer 5, which is coupled to the bus directly after the interface assembly, in order to monitor the bus datastream. This measure ensures that the safety analyzer can monitor the entire input datastream as well as the entire output datastream on the bus, when connected to a serial bus with a ring structure. The safety analyzer 5 uses the knowledge of the entire datastream via the bus to store the complete process map in a memory provided for this purpose, in the described embodiment. In consequence, the safety analyzer is able to check all the safety-related logic linking data for the safety-related control system in the interface assembly and, if necessary, that is to say when a fault occurs, to drive the output 6 to switch the entire system off by means of the contactor 7 on a safety basis, such that the supply voltage is switched off for the entire system.

**[0043]** The automation system according to the invention in Fig. 3 shows a modification of

the embodiment illustrated in Fig. 2. In this case, the safety analyzer 5 is integrated in the interface assembly 41. The safety-related control of the standard control device and the safety-related data processing in the safety analyzer run in separate and independent logic modules in the interface assembly. Furthermore, a second safety analyzer 5'' is arranged at the head of the local bus spur 8. This arrangement is in turn dependent on the safety analyzer 5'' being able to monitor all the input data and output data for the subscribers 33, 34 and 35 on the local bus spur 8 and, accordingly, of being able to apply a complete process map for the process sequence within the local bus spur. Like the safety analyzer 5 in the long-distance bus section, the safety analyzer 5'' is thus able to check all the safety-related logic linking data for the safety-related control system for the local bus section in the interface assembly and, if necessary and as described above, to initiate the necessary safety-related functions by data manipulation. This allows very stringent safety requirements which are placed on the safety-relevant inputs and outputs applicable to the bus spur 8 to be satisfied, since the local bus spur 8 is protected not only by the safety-related control of the standard control device, but also by the safety analyzer 5 and by the safety analyzer 5''.

**[0044]** Fig. 4 shows a further embodiment of the invention. The automation system according to the invention has two safety analyzers 5 and 5', whose safety-related outputs 6 and 6' are coupled to one another. Both outputs control a multiple contactor device 7 for switching off the supply voltage for the entire system. The system is controlled via a standard control device 4 via the serial bus 2. Since it is arranged in the system, the safety analyzer 5 can monitor all the input and output data on the bus, except for the input data for the first bus subscriber 31, which is arranged between the control device 4 and the

safety analyzer 5. The safety analyzer 5' can monitor all the input data on the bus, but none of the output data except for that for the last bus subscriber is accessible to it. By copying the relevant data in the bus data flow, the first safety analyzer 5 is therefore able to copy the output data accessible to it into input data and thus to make available to the safety analyzer 5' as well the output data, which is actually not accessible to said safety analyzer 5', for application of a process map for the safety-related bus subscriber 32 to be protected. Since both safety analyzers receive the same input information, they can monitor the safety-related inputs and outputs of the bus subscriber 32 to be protected. This provides distributed redundancy for the safety technology in the automation system according to the invention. In the present example, the safety analyzer 5' also has a safety-related input 10, to which an emergency switch 13 is connected. When the emergency switch 13 is closed, the safety analyzer 5' responds with the associated safety-related function in the safety analyzer, namely the opening of the contactor 7 in order to switch off the entire system.

**[0045]** The described method for copying input data into output data, and vice versa, is also used, according to the invention, to provide a data link between two slaves in the automation system operating on the master-slave principle, without the master being required for data transmission. In this case, for example, a safety analyzer which is associated with one bus subscriber can insert the data item to be transmitted for the bus subscriber into the input datastream, and thus make it available to a downstream bus subscriber, without involving the master. In this way, if required, information can be multicast or broadcast in a simple manner to all the other downstream bus subscribers.

**[0046]** In one embodiment of the invention, which is not illustrated, the safety analyzer is

integrated in an associated safety-based bus subscriber. The safety-based logic links are in this case provided in a logic unit in the bus subscriber, so that intelligence installed in the bus subscriber can be used for the safety-based logic links. Since the bus subscriber has a bus interface, this considerably reduces the additional hardware complexity for the safety analyzer.

[0047] At least in some cases, the safety-related data is transmitted via the bus using a security protocol for data transmission in the described automation systems according to the invention. Depending on the requirement, this security protocol may include, in addition to the safety data item, the negated safety data item, and an address and/or data protection information in the form of a CRC. This allows errors during data transmission to be identified easily. For this purpose, a safety analyzer which is used in the automation system according to the invention is set up such that it can read the security protocol, and can evaluate it appropriately.

[0048] The address of the safety bus subscriber transmitted in the security protocol allows the safety analyzer to adapt the programming, to identify the data set of the subscriber associated with it, and to take account of the change in the bus layout when the bus layout is changed, for example as a result of the component being switched off for safety reasons. In addition, the inclusion of the address in the security protocol allows a storage error caused by a bus fault or a failure in the decentralized unit to be detected.

[0049] One particular embodiment of a safety analyzer for use in the automation system according to the invention is shown in Fig. 5. The illustrated safety analyzer 5 has not only four safety-based inputs 10 for detecting safety-based information from photodetectors 11, but also four safety-based outputs 6 for disconnecting the supply

**[0051]** It should furthermore be stated that the principle of the invention is not restricted to the automation bus systems described in the exemplary embodiments but, in fact, can be applied to all automation systems having a bus.



Docket No.  
(H)01PH0419USP

# Declaration and Power of Attorney For Patent Application

## English Language Declaration

As a below named inventor, I hereby declare that:

My residence, post office address and citizenship are as stated below next to my name,

I believe I am the original, first and sole inventor (if only one name is listed below) or an original, first and joint inventor (if plural names are listed below) of the subject matter which is claimed and for which a patent is sought on the invention entitled  
**Safety-Related Automation Bus System**

the specification of which

(check one)

☐ is attached hereto.

☒ was filed on June 16, 2000 as United States Application No. or PCT International  
Application Number PCT/DE00/01901  
and was amended on \_\_\_\_\_

(if applicable)

I hereby state that I have reviewed and understand the contents of the above identified specification, including the claims, as amended by any amendment referred to above.

I acknowledge the duty to disclose to the United States Patent and Trademark Office all information known to me to be material to patentability as defined in Title 37, Code of Federal Regulations, Section 1.56.

I hereby claim foreign priority benefits under Title 35, United States Code, Section 119(a)-(d) or Section 365(b) of any foreign application(s) for patent or inventor's certificate, or Section 365(a) of any PCT International application which designated at least one country other than the United States, listed below and have also identified below, by checking the box, any foreign application for patent or inventor's certificate or PCT International application having a filing date before that of the application on which priority is claimed.

Prior Foreign Application(s)

Priority Not Claimed

199 27 635.8

(Number)

Germany

(Country)

17 June 1999

(Day/Month/Year Filed)

☐

(Number)

(Country)

(Day/Month/Year Filed)

☐

(Number)

(Country)

(Day/Month/Year Filed)

☐

I hereby claim the benefit under 35 U.S.C. Section 119(e) of any United States provisional application(s) listed below:

\_\_\_\_\_  
(Application Serial No.)

\_\_\_\_\_  
(Filing Date)

\_\_\_\_\_  
(Application Serial No.)

\_\_\_\_\_  
(Filing Date)

\_\_\_\_\_  
(Application Serial No.)

\_\_\_\_\_  
(Filing Date)

I hereby claim the benefit under 35 U. S. C. Section 120 of any United States application(s), or Section 365(c) of any PCT International application designating the United States, listed below and, insofar as the subject matter of each of the claims of this application is not disclosed in the prior United States or PCT International application in the manner provided by the first paragraph of 35 U.S.C. Section 112, I acknowledge the duty to disclose to the United States Patent and Trademark Office all information known to me to be material to patentability as defined in Title 37, C. F. R., Section 1.56 which became available between the filing date of the prior application and the national or PCT International filing date of this application:

\_\_\_\_\_  
(Application Serial No.)

\_\_\_\_\_  
(Filing Date)

\_\_\_\_\_  
(Status)  
(patented, pending, abandoned)

\_\_\_\_\_  
(Application Serial No.)

\_\_\_\_\_  
(Filing Date)

\_\_\_\_\_  
(Status)  
(patented, pending, abandoned)

\_\_\_\_\_  
(Application Serial No.)

\_\_\_\_\_  
(Filing Date)

\_\_\_\_\_  
(Status)  
(patented, pending, abandoned)

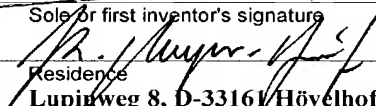
I hereby declare that all statements made herein of my own knowledge are true and that all statements made on information and belief are believed to be true; and further that these statements were made with the knowledge that willful false statements and the like so made are punishable by fine or imprisonment, or both, under Section 1001 of Title 18 of the United States Code and that such willful false statements may jeopardize the validity of the application or any patent issued thereon.

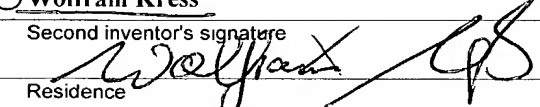
POWER OF ATTORNEY: As a named inventor, I hereby appoint the following attorney(s) and/or agent(s) to prosecute this application and transact all business in the Patent and Trademark Office connected therewith. (list name and registration number)

M. Robert Kestenbaum Reg. No. 20,430

Send Correspondence to: M. Robert Kestenbaum  
11011 Bermuda Dunes NE  
Albuquerque, NM USA 87111

Direct Telephone Calls to: (name and telephone number)  
M. Robert Kestenbaum (505) 323-0771 Fax (505) 323-0865

1-00	Full name of sole or first inventor <b>Karsten Meyer-Gräfe</b>	
	Sole or first inventor's signature 	Date 20.03.02
	Residence <b>Lupinweg 8, D-33161 Hövelhof, Germany</b>	
	Citizenship <b>German</b> <b>DEX</b>	
	Post Office Address <b>Lupinweg 8, D-33161 Hövelhof, Germany</b>	

2-00	Full name of second inventor, if any <b>Wolfram Kress</b>	
	Second inventor's signature 	Date 26.03.02
	Residence <b>Auf dem Gerotten 16, D-53721 Siegburg, Germany</b>	
	Citizenship <b>German</b> <b>DEX</b>	
	Post Office Address <b>Auf dem Gerotten 16, D-53721 Siegburg, Germany</b>	